UNIVERSIDAD DE EL SALVADOR
FACULTAD MULTIDISCIPLINARIA PARACENTRAL
DEPARTAMENTO DE INFORMÁTICA
INGENIERÍA DE SISTEMAS INFORMÁTICOS

SOFTWARE DINAMICO PARA LA EVALUACION DE LA SEGURIDAD DE LAS BASES DE DATOS Y REDES INFORMATICAS EN INSTITUCIONES PUBLICAS, PRIVADAS Y NO GUBERNAMENTALES DEL DEPARTAMENTO DE SAN VICENTE

PRESENTADA POR:
AYALA GUARDADO, EVELYN XIOMARA
FLORES IRAHETA, SANDRA GUADALUPE
HERNÁNDEZ FERNÁNDEZ, SULMA DOLORES

PARA OPTAR AL TITULO DE:
INGENIERO DE SISTEMAS INFORMÁTICOS

SAN VICENTE, MAYO DE 2015

UNIVERSIDAD DE EL SALVADOR

RECTOR:

Ing. Mario Roberto Nieto Lovo

SECRETARIA GENERAL:

Dra. Ana Leticia Zavaleta de Amaya

FACULTAD MULTIDISCIPLINARIA PARACENTRAL

DECANO:

Ing. MSc. José Isidro Vargas Cañas

SECRETARIO (A):

Lic. MSc. José Martin Montoya Polío

DEPARTAMENTO DE INFORMÁTICA

JEFE:

Lic. MSc. José Oscar Peraza

UNIVERSIDAD DE EL SALVADOR
FACULTAD MULTIDISCIPLINARIA PARACENTRAL
DEPARTAMENTO DE INFORMÁTICA

Trabajo de Graduación previo a la opción al grado de:
INGENIERO DE SISTEMAS INFORMÁTICOS

Título:

SOFTWARE DINAMICO PARA LA EVALUACION DE LA SEGURIDAD DE LAS BASES DE DATOS Y REDES INFORMATICAS EN INSTITUCIONES PUBLICAS, PRIVADAS Y NO GUBERNAMENTALES DEL DEPARTAMENTO DE SAN VICENTE

Presentado por:
AYALA GUARDADO, EVELYN XIOMARA
FLORES IRAHETA, SANDRA GUADALUPE
HERNÁNDEZ FERNÁNDEZ, SULMA DOLORES

Trabajo de Graduación aprobado por:

DOCENTE COORDINADOR:
ING. ANA BEATRIZ AGUIRRE

DOCENTE ASESOR:
ING. RENÉ WILBERTO RIVERA COREAS

San Vicente, mayo de 2015

Trabajo de Graduación Aprobado por:

Docentes Directores:

ING. ANA BEATRIZ AGUIRRE

ING. RENÉ WILBERTO RIVERA COREAS

AGRADECIMIENTOS

UNIVERSIDAD DE EL SALVADOR

Por ofrecer una alternativa de desarrollo profesional de alto prestigio y con fundamentos educativos de calidad y un alto nivel de ética profesional.

FACULTAD MULTIDISCIPLINARIA PARACENTRAL

Por brindar una opción de educación superior de alto prestigio y accesible para los jóvenes de la zona paracentral.

DEPARTAMENTO DE INFORMÁTICA

Por proporcionar la coordinación adecuada para formarnos en las diferentes áreas de conocimientos requeridas para la carrera de sistemas informáticos por medio de la planta docente que lo conforma.

DOCENTES DIRECTORES

ING. ANA BEATRIZ AGUIRRE, ING. RENÉ WILBERTO RIVERA COREAS

Por su valioso tiempo brindado durante el proceso de asesorías para lograr la culminación de este proyecto.

AYALA GUARDADO, EVELYN XIOMARA

FLORES IRAHETA, SANDRA GUADALUPE

HERNÁNDEZ FERNÁNDEZ, SULMA DOLORES

AGRADECIMIENTOS

En primer lugar doy gracias a DIOS por regalarme la fortaleza para llegar hasta el final de mi carrera, en él encontré el sostén que me ayudo a continuar en mis momentos difíciles en esas noches incontables de cansancio y desvelo, en esos momentos duros en los que creía que la salida era renunciar, fue el quien me regalo paciencia, constancia, entendimiento y fortaleza para superar todos los obstáculos y llegar hasta aquí.

Doy gracias a mis padres Doris Elizabeth Guardado de Ayala y Humberto Ayala Ramírez por haberme regalado el apoyo moral y económico para poder hacer realidad este proyecto, en especial a mi madre por haberme acompañado en mis momentos difíciles y brindado palabras de ánimo cuando más las necesite.

Agradezco a dos personas que quiero mucho, mis hermanos Humberto Gehovany Ayala Guardado y Johana Elizabeth Ayala Guardado por ser mi alegría e inspiración para lograr esta meta.

A mi familia en general especialmente a mi tía y amiga María Lucila Ayala por estar muy pendiente de mí durante este proceso y haberme regalado sus consejos y su apoyo incondicional.

A mis amigas y compañeras de tesis por haberse mantenido constantes en nuestro objetivo en común a pesar de las adversidades que afrontamos como grupo, por todos los momentos de alegrías y tristezas que vivimos juntas y por el apoyo mutuo que nos dimos en los momentos difíciles.

A los docentes en general por haber sido parte fundamental en el proceso de aprendizaje durante todo el transcurso de la carrera en especial a ing. Yancy Molina, ing. Virna Urquilla, Ing., Herbert Monge, Lic. Adalton Carranza y al lic. Oscar Peraza quienes tienen mi admiración y respeto por la gran labor que desempeñan.

AYALA GUARDADO, EVELYN XIOMARA

AGRADECIMIENTOS

Agradezco primeramente a Dios ya que él es el que me dio fortaleza, salud y vida para poder terminar mi carrera y así poder ser una profesional, como también en los momentos más difíciles él estuvo ahí para darme sanidad y fuerzas para levantarme y así seguir adelante, es por eso que a él le debo mi felicidad.

Este triunfo también se lo debo a mis padres Carmen Iraheta y Gilberto Flores quienes con mucho esfuerzo y con la ayuda de Dios y la Santísima Virgen me brindaron lo necesario para que pudiera superarme ya que son ellos los que siempre estuvieron a mi lado apoyándome, aconsejándome y dándome ánimos para no decaer, por lo tanto este triunfo también es de ellos por eso les agradezco mucho y le doy gracias a Dios por darme unos padres tan hermosos y únicos.

Agradezco a mis hermanos, Carlos Flores y Luis Flores y mis hermanas, Deysi Flores, Xenia Flores, Yaneth Flores y Claudia Iraheta, quienes siempre estuvieron apoyándome en las buenas y en las malas durante el trayecto de mi carrera como buenos hermanos/as.

A una persona muy especial para mí, Fernando Ruíz por encomendarme en sus oraciones y brindarme su apoyo, e igual a mi mejor amiga Genoveva Cubías a quien quiero mucho y siempre le estaré agradecida.

A mi grupo de tesis Xiomara Ayala y Sulma Hernández con las que compartí muchas cosas buenas y malas pero que siempre a pesar de los inconvenientes estuvimos unidas y trabajando como un gran equipo, agradezco a ellas que son unas grandes amigas y que tuvieron paciencia y comprensión hacia mi persona en algunas ocasiones y por la dedicación que mostraron en el transcurso del desarrollo de nuestra tesis.

A mis amigos por brindarme su apoyo incondicional gracias.

A los docentes en general que fueron parte de mi formación profesional les doy las gracias por los conocimientos que me brindaron ya que a través de ellos contribuyeron al logro de mi gran objetivo.

FLORES IRAHETA, SANDRA GUADALUPE

AGRADECIMIENTOS

En primer lugar a Dios por darme el don maravilloso de la vida, la sabiduría, la salud, por guiarme en cada uno de mis pasos.

A mi padre Manuel de Jesús Hernández y especialmente a mi madre Rosa Esmeralda Fernández Castro y a mi tía Blanca Edilia Hernández que son ellas las que han estado en cada momento de mi vida, brindándome cariño, comprensión, consejos y apoyo incondicional.

A mis hermanos Ángel Edenílson, Maricela Azucena y Elsa Noemí, por haberme apoyado y animado siempre en el trayecto de mi carrera; A mis sobrinos: Esmeraldita, Nataly, Josue y Néstor. A mis primos en especial a Haydee, tíos y familiares que sé que han estado ahí constantes con sus oraciones y palabras de ánimo para apoyarme a seguir adelante.

A mi amado esposo Josué López por haber estado a mi lado como Novio y ahora esposo motivándome a no rendirme, por haber sido tan compresivo y amoroso en esos momentos difíciles.

A mis compañeras de Trabajo de Graduación Sandra Flores y Xiomara Ayala porque a pesar de los momentos difíciles nunca nos dimos por vencidas, sé que cada sacrificio, también fue acompañado de momentos hermosos, que de no haber sido por este trabajo de graduación difícilmente los hubiéramos compartido.

A todos mis amigos en especial a Daniel López, Idalia Reyes y a mi jefe El señor Jaime Galileo Chávez a los cuales agradezco su apoyo incondicional.

A todos los docentes del Departamento de Informática por ser parte esencial en mi formación profesional, en especial a los responsables del Proceso de Graduación: Ing. René Wilberto Rivera Coreas e Ing. Ana Beatriz Aguirre.

HERNÁNDEZ FERNÁNDEZ, SULMA DOLORES

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad la tecnología va avanzando considerablemente, por lo que muchas de las Instituciones hoy en día se ven en la necesidad de manejar la información por medios electrónicos para agilizar los procesos, es por esta razón que el personal encargado del manejo de bases de datos y redes informáticas necesita estar actualizándose periódicamente respecto a la administración de seguridad en el manejo de información.

En el presente trabajo en primer lugar se da a conocer los objetivos que se pretenden alcanzar y la justificación respectiva de dicha investigación, además se detallan los alcances y limitaciones que tendría el desarrollo del proyecto. El contenido de este trabajo está dividido en cinco capítulos:

Capítulo I muestra el estudio preliminar realizado en donde se da a conocer un poco sobre los orígenes de la seguridad informática, y de qué manera esta temática ha crecido en nuestro país; luego se identifica la situación problemática a la que se enfrentan actualmente las instituciones públicas, privadas y no gubernamentales del departamento de San Vicente, analizando cuatro áreas principales las cuales son: niveles de seguridad por parte de los usuarios, niveles de seguridad en los equipos informáticos, niveles de seguridad físicos y niveles de seguridad en el manejo de la información; definiendo así el problema por medio del diagrama causa-efecto (Ishikawa).

Además se plasmó el sistema de hipótesis a comprobar y la metodología utilizada para recolectar información. Así mismo se estableció la muestra y la población con la que se trabajó, y los recursos necesarios para el desarrollo de la investigación y del software, así como el análisis de las factibilidades respectivas.

Capítulo II muestra los fundamentos teóricos de la investigación, es decir; el marco teórico en el cual se describen los términos esenciales que definen la seguridad en bases de datos y redes informáticas.

Capítulo III se da a conocer la recolección, presentación y análisis de la información.

Capítulo IV muestra la prueba de hipótesis, es decir; la descripción y aplicación de la prueba de hipótesis, junto con sus respectivas conclusiones e interpretación de los resultados de la prueba estadística.

Finalmente el Capítulo V muestra la etapa de desarrollo, la cual comprendió la definición de los requerimientos, la descripción de la metodología, el diseño de la base de datos del software y las interfaces de la propuesta diseñada en la cual se aplicó los resultados de la investigación realizada para crear un software dinámico para la evaluación de la seguridad de las bases de datos y redes informáticas en instituciones públicas, privadas y no gubernamentales del departamento de San Vicente.

En la elaboración del software no se tomó en cuenta su implementación, ni el resultado que dicho software proporcione ya que será en base a la información ingresada por las empresas, instituciones y organizaciones que hagan uso de él.

OBJETIVOS DEL PROYECTO

OBJETIVO GENERAL

Contribuir a la mejora de la seguridad de las bases de datos y redes informáticas de instituciones públicas, privadas y no gubernamentales del departamento de San Vicente, por medio de un software dinámico que permita medir el nivel de seguridad con que se resguardan sus datos.

OBJETIVOS ESPECÍFICOS

- Determinar la condición actual de la seguridad de bases de datos utilizadas por las instituciones públicas, privadas y no gubernamentales del departamento de San Vicente.

- Proporcionar medidas de seguridad física para minimizar la vulnerabilidad ante riesgos, en las bases de datos y redes informáticas de las instituciones públicas, privadas y no gubernamentales del departamento de San Vicente.

- Proponer medidas preventivas y correctivas de seguridad lógica para las bases de datos y redes informáticas de las instituciones públicas, privadas y no gubernamentales del departamento de San Vicente.

JUSTIFICACIÓN

Las instituciones públicas, privadas y no gubernamentales de El Salvador se ven cada vez más en la necesidad de administrar mayores volúmenes de información debido a la creciente demanda de servicios, esta información tiene que ser manejada de forma segura, permitiendo el fácil acceso, de tal manera que se puedan tomar decisiones y mostrar informes en el momento oportuno.

Algunas instituciones conocen los beneficios de manejar bases de datos digitales, pero aún no superan la barrera de la inseguridad, ya sea por la escases de recursos, de tiempo o dinero para poder instruir a su personal en el área de informática y así suplir la necesidad de conocimiento y superar los problemas de inseguridad, estos problemas fueron identificados por medio del sondeo realizado con la encuesta "Seguridad de la información" (ver anexo N° 3, pág. 235), con la cual se determinaron cuatro áreas de mayor incidencia las cuales son: **Nivel de seguridad por parte de los usuarios**, en el cual se identificó la problemática de personal no capacitado, ausencia de administradores, uso de páginas de descargas no autorizadas, entre otros. En **el nivel de seguridad en los equipos informáticos** se detectó que en muchos casos el equipo está incompleto, posee fallos o no se hace el uso apropiado de él. En **el nivel de seguridad física** se identificó la vulnerabilidad en el acceso a la red, mala ubicación del equipo y en **el nivel de seguridad del manejo de la información** se identificó contraseñas compartidas, accesos no deseados entre otros. Agregando a esto que las instituciones contaban con información que en muchos casos debía ser expuesta al público y se necesitaba garantizar la integridad y veracidad de dicha información, evitando que esta fuera modificada o manipulada de forma inapropiada por personas que no estaba autorizadas para realizar dichos eventos.

Es por ello que se identificó la necesidad de brindarle a las instituciones medidas de seguridad que mejoran la protección de su información, desde el acceso a la red, la protección contra perdida hasta la infiltración en las bases de datos, para proteger del hurto o de la manipulación inadecuada.

Según el Consejo Nacional de Ciencia y Tecnología, en los Indicadores de Ciencia y Tecnología del año 2011 el 63.16% de las Instituciones de El Salvador contaban con un sistema informático al que se puede acceder desde lugares fuera de la institución además, se representa un crecimiento significativo en cuanto al acceso de las bases de datos entre el año 2009 al 2011. (Marroquín y otros, 212, p. 54)

La problemática de la inseguridad de la información en bases de datos y redes informáticas se abordó de manera que permitiera minimizar la incidencia y que garantizara la seguridad de la información, para esto se concientizo a los responsables de la manipulación de esta, para que comprendieran los riesgos que se corren al efectuar malos procedimientos o violentar políticas de protección a la información, de manera general que tengan conciencia de cuál es el nivel de seguridad con que resguardan la información y como pueden mejorarla en caso que lo necesiten. Con la investigación realizada se pretende brindar un aporte significativo sobre la seguridad de las bases de datos y redes informáticas en instituciones públicas, privadas y no gubernamentales del departamento de San Vicente, para lo cual se recopilará, estudiará y diseñarán formas de proteger la información de las instituciones y prevenir la infiltración de intrusos a las redes, como también se brindan las medidas de seguridad que se deben tomar para disminuir la vulnerabilidad en la seguridad de bases de datos y redes informáticas todo esto integrado en un software de fácil utilización y de acceso gratuito el cual ayudará a mejorar la seguridad de las instituciones antes mencionadas.

El software que se elaboró permite interactuar con el usuario, al solicitarle los datos propios referentes a la forma en que manipula la información la institución que está siendo evaluada, lo que se aporta al software los valores que son comparados con los resultados obtenidos y almacenados previamente de la investigación realizada, para poder arrojar la evaluación del nivel de seguridad que posee la institución.

En la investigación nos enfrentamos a situaciones donde la información fue difícil de recopilar; por lo que se aplicaron diversas técnicas que facilitaron la recolección de la información, tales como: Observación sistemática, observación participante, encuestas, entre otras que nos brindaron la oportunidad de obtener la información necesaria.

Esta investigación se llevó a cabo en el departamento de San Vicente, seleccionando de él, los cuatro municipios con mayor número de unidades económicas, según los datos mostrados por la DIGESTYC (ver anexo N° 1, pág. 229). Siendo estos los siguientes, San Vicente, Tecoluca, San Sebastián y Apastepeque, beneficiando a instituciones públicas, empresas privadas y no gubernamentales, como también a los estudiantes de la Universidad de El Salvador que necesiten retomar información del tema para futuras investigaciones. Además con el software desarrollado se beneficiarán a dichas instituciones, contribuyendo de manera significativa a la mejora de la seguridad de las bases de datos y redes informáticas.

ALCANCES DEL PROYECTO

- **Definición de expectativas y métricas de seguridad de bases de datos y redes informáticas**

  Se Identificaron los conceptos básicos de seguridad de bases de datos y redes informáticas, las métricas por medio de las cuales se pudo considerar si las instituciones alcanzan las expectativas de seguridad.

- **Controles de tipo físico**

  Se diseñaron medidas generales de seguridad para el acceso a las instalaciones y condiciones infraestructurales y ambientales que contribuyan a la seguridad de las bases de datos.

- **Políticas de seguridad de las empresas**

  Se analizó si las instituciones del departamento de San Vicente implementan políticas para la protección de datos.

- **Determinación de medidas de seguridad para información pública y privada**

  Se realizó un análisis de lineamientos que utilizan las Instituciones del departamento de San Vicente para resguardar de forma segura información pública y privada.

- **Medidas de seguridad en redes**

  Se determinó las medidas de seguridad de las redes informáticas y si en las instituciones del departamento de San Vicente se están implementando medidas para proteger las bases de datos distribuidas o con acceso por internet e intranet.

- **Identificación de amenazas más comunes**

  Por medio del estudio se determinó cuáles son las amenazas más comunes que atentan contra la seguridad de las bases de datos del departamento de San Vicente.

- **Selección y planificación de las medidas mitigadoras (estrategias)**

  Identificadas las amenazas se plantearon medidas generales que ayuden a mitigarlas.

- **Diseño de software**

  Elaboración de un software dinámico que evalué el nivel de seguridad con el que resguardan la información las instituciones que poseen bases de datos, por medio de parámetros proporcionados por el usuario que permitan ser comparados con los parámetros del software previamente obtenidos por la investigación realizada, para determinar el nivel de seguridad con el que están manejando sus datos y poder identificar las posibles debilidades y fortalezas en la seguridad de las redes y bases de datos.

  El software dinámico proporciona los resultados de la evaluación por medio de criterios calificativos que indiquen la calidad de la seguridad implementada para resguardar la información.

  En la elaboración del software no se tomó en cuenta su implantación, y el resultado que dicho software proporcione será en base a la información ingresada por las empresas, instituciones y organizaciones que hagan uso de él.

  El desarrollo del software comprende:

  - Diseño de pantallas de entradas.
  - Diseño de pantallas de salidas.
  - Diseño de la base de datos

LIMITACIONES DEL PROYECTO

- Riesgos en el acceso a zonas con presencias delincuencial que dificulten la recolección de información.

- Inseguridad en cuanto a la veracidad de la información obtenida por parte de las personas.

CAPÍTULO I. ESTUDIO PRELIMINAR.

Síntesis.

En este capítulo se presenta la información utilizada para el desarrollo de la investigación considerando el planteamiento del problema, la redacción de hipótesis generales y específicas con su respectiva operacionalización de variables, así como también la descripción del tipo, método y diseño de investigación, además se determina la población y la muestra en estudio y las factibilidades técnica, operativa y económica-social.

1.1. PLANTEAMIENTO DEL PROBLEMA

1.1.1. Antecedentes del problema

Desde hace mucho tiempo en la historia el hombre ha tenido la necesidad de almacenar información en medios tales como: piedra, piel, madera, papel, cintas magnéticas, discos entre otros, buscando siempre que estos medios sean seguros debido a la importancia que la información almacenada en ellos representa.

Pero el creciente aumento en la tecnología, en la cantidad de datos manipulados por empresas e instituciones y la manipulación de los datos en sistemas en red ha vuelto cada vez más difícil el trabajo en cuanto a seguridad informática.

Cada día existen nuevos casos y nuevas formas de inseguridad en los datos almacenados en redes informáticas, como los dados a conocer en la investigación realizada por la Universidad de El Salvador para el año 2008 titulada " Estudio y análisis sobre la informática forense en El Salvador", expresa que para el año 2007 en nuestro país la defensoría del consumidor contaba con 3 casos en los cuales la información de las cuentas bancarias de las personas había sido accedida de manera ilegal por medio de clonación de tarjetas de crédito. (Belloso, 2008, p. 262).

En el mismo estudio también se dio a conocer la encuesta realizada a 10 jueces del país, donde 6 de ellos opinan que un 22% de los problemas de inseguridad informática lo enfrentan aquellas personas cuyas instituciones bancarias no les ofrecen una garantía en cuanto a la autenticidad de los datos que prevengan la clonación de tarjetas.

Además según la experiencia y conocimiento de dichos jueces, en cuanto a problemas de seguridad informática, dos de ellos opinan que existen casos de robo de información confidencial. (Belloso, 2008, p. 117).

En la misma investigación la División de Informática de INTERPOL, dio a conocer los casos investigados en los cuales ha sido violada la seguridad informática de instituciones o empresas en el período comprendido de junio de 2005 a diciembre de 2007:

1- Caso de hacking 01/08/2006.
2 -Casos de estafas electrónicas en fechas 20/12/2006, 04/01/2007

En el año 2008 la Universidad Tecnológica de El Salvador realizó un diseño sobre seguridad informática titulado “Diseño de un modelo de seguridad informática, basado en estrategias de hardware y software para ser aplicado en empresas de mediana escala” en su modelo proponen el análisis de elementos fundamentales para mantener la seguridad informática en una empresa tales como: Infraestructura, software, hardware, medidas de seguridad, entre otros.

Para el año 2007 la empresa llamada Sistemas Eficientes, S.A abreviada SEFISA especializada en seguridad, realizó una investigación titulada “Robo de Información” dirigida por Erick Fortin gerente de tecnología, dio a conocer en el resultado de su investigación que la mayor amenaza a la seguridad general de las organizaciones de El Salvador es en un 52% la filtración de información confidencial/patentada.

Definieron otros problemas de seguridad en bases de datos y redes informáticas que enfrentan las instituciones: Virus, interrupción de servicios, intercepción y modificación de información, intercepción de wireless, robo o extravío de notebooks, agujeros de seguridad de redes conectadas.

Existen investigaciones orientas hacia la seguridad informática de manera generalizada, pero no así en las que se trate de manera específica la seguridad de las bases de datos o de las redes informáticas.

Situación Problemática

Con la investigación preliminar realizada se identificó que en el departamento de San Vicente las instituciones públicas, privadas y no gubernamentales que almacenan su información en bases de datos se encontraban expuestas a diversas situaciones que ponían en riesgo su información ya sea a pequeña o gran escala, sufriendo pérdidas de información o la integridad de esta, que podrían ser temporales, permanentes e irremediables si no se contaba con las medidas preventivas y correctivas suficientes, en esta problemática, se identificó inmersos muchos elementos que afectaban, entre ellos podemos mencionar:

- La ausencia de administradores de bases de datos o la asignación del cargo a personas que no son profesionales en el área.
- Las condiciones del equipo utilizado para almacenar los datos.
- La red con ausencia de protocolos de seguridad.
- La desactualización de conocimientos informáticos del personal encargado del uso de los sistemas que almacenan la información.
- La ausencia de las medidas de seguridad física, entre otros elementos que influyen en la seguridad.

En grandes rasgos estos son los elementos que se consideraron para garantizar niveles aceptables de seguridad, pero para las empresas que aún están en desarrollo y no cuentan con la estabilidad y recursos suficientes para contratar a expertos en el área o para proporcionar cursos completos, integrales y que garanticen el aprendizaje de sus empleados, es necesaria una herramienta de fácil utilización, que retome todos estos elementos y pueda evaluar el nivel de seguridad de la información proporcionando las medidas más oportunas para los casos que presenten deficiencia, la problemática se abordó únicamente para las instituciones públicas, empresas privadas y no gubernamentales, contribuyendo a mejorar la seguridad de su información.

Para conocer la problemática en cuanto al nivel de seguridad que manejaban las instituciones públicas, privadas y no gubernamentales del departamento de San Vicente, se realizó un estudio preliminar haciendo uso de la encuesta denominada “Encuesta sobre seguridad de la información” (ver anexo N° 3, pág. 235), aplicada en los cuatro municipios del departamento con mayor número de unidades económicas siendo estos: San Vicente,

Tecoluca, San Sebastián y Apastepeque; teniendo en cuenta que estos municipios tienen el mayor número de empresas e instituciones, y son los que conformaron nuestra población en estudio.

El número de instituciones estudiadas por municipio se detalla en la tabla siguiente:

Tabla 1: Número de instituciones por municipio

Municipios	Instituciones públicas	Empresas privadas	ONG's	Población Total
Apastepeque	6	1	0	7
San Sebastián	4	3	0	7
San Vicente	27	51	6	84
Tecoluca	5	3	2	10
Total población	42	58	8	**108**

Fuente: Investigación realizada

El factor a considerar para las instituciones estudiadas fue que estas tuvieran un sistema informático por medio del cual se manejara el registro de información.

El estudio se dividió en cuatro áreas que se consideraron como las más influyentes en el manejo de la seguridad:

- Niveles de seguridad por parte de los usuarios.
- Niveles de seguridad en los equipos informáticos.
- Niveles de seguridad físicos.
- Niveles de seguridad en el manejo de información.

Los resultados obtenidos fueron los siguientes:

- **Niveles de seguridad por parte de los usuarios**

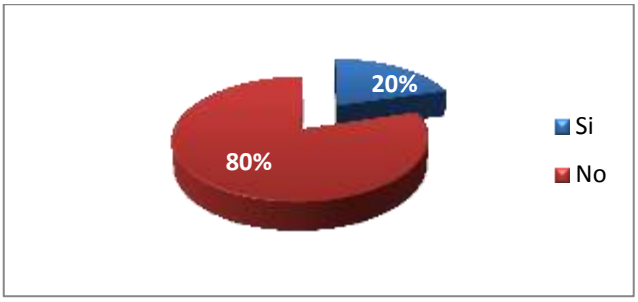
De las 108 instituciones solo un 20% de ellas contaba con uno o más administradores internos, se pudo observar que en la mayoría de instituciones el volumen de información manejada, el número de equipo utilizado era considerable y que varias de las que no contaban con un administrador informático no era porque no lo necesitaran si no por otros factores que serán desglosados en la descripción del diagrama de causa-efecto. El resultado de este análisis se muestra en la gráfica siguiente:

Tabla 2: Instituciones con administrador informático interno

Cuentan con administrador informático	Instituciones	%
SI	22	20%
No	86	80%

Fuente: Elaboración propia

Gráfica 1: Instituciones que cuentan con administrador informático



Fuente: Elaboración propia

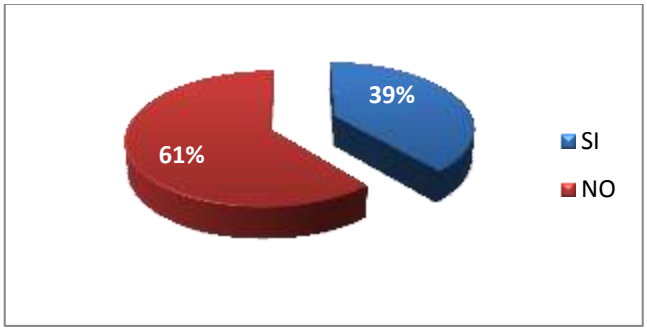
En el 61% de las instituciones el personal no había sido capacitado en los últimos dos años. Ver gráfica siguiente:

Tabla 3: Instituciones con personal no capacitado

Capacitaciones	Instituciones	%
SI	42	39%
NO	66	61%

Fuente: Elaboración propia

Gráfica 2: Capacitaciones de computación



Fuente: Elaboración propia

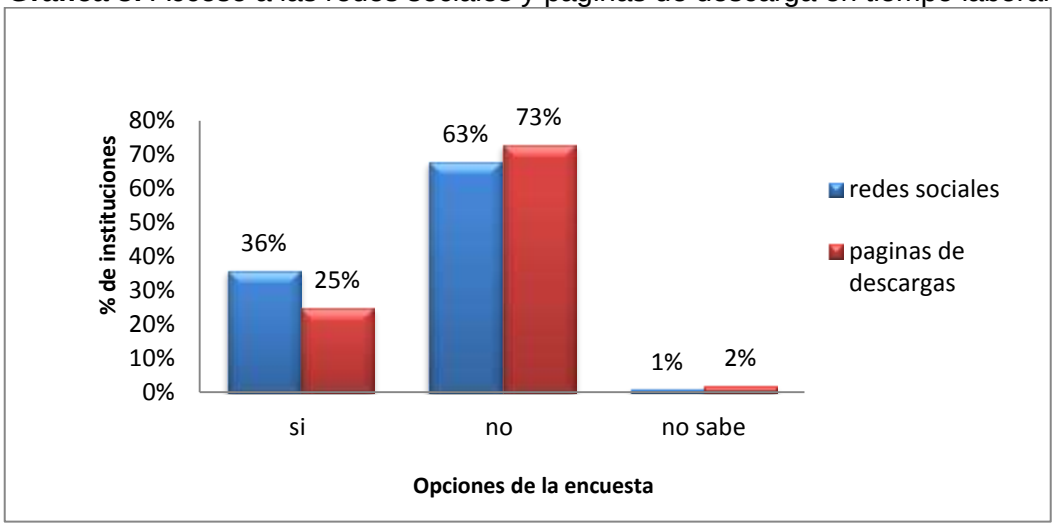
El 25% de las instituciones tenían acceso a páginas de descarga y el 36% tenían acceso a redes sociales, de igual forma algunos encuestados afirmaron que lograron acceder a dichas páginas por medios no autorizados. Ver gráfica siguiente:

Tabla 4: Instituciones con accesos a páginas de descarga y redes sociales

Opciones de cuestionario	Redes sociales	%	Páginas de descargas	%
SI	39	36%	27	25%
NO	68	63%	79	73%
No sabe	1	1%	2	2%

Fuente: Elaboración propia

Gráfica 3: Acceso a las redes sociales y páginas de descarga en tiempo laboral



Fuente: Elaboración propia

- **Nivel de seguridad en el equipo**

El rendimiento del equipo informático puede verse afectado debido a las siguientes causas:

- Saturación de procesos
- Infección por virus
- Sobrecarga de archivos
- Falta de mantenimiento

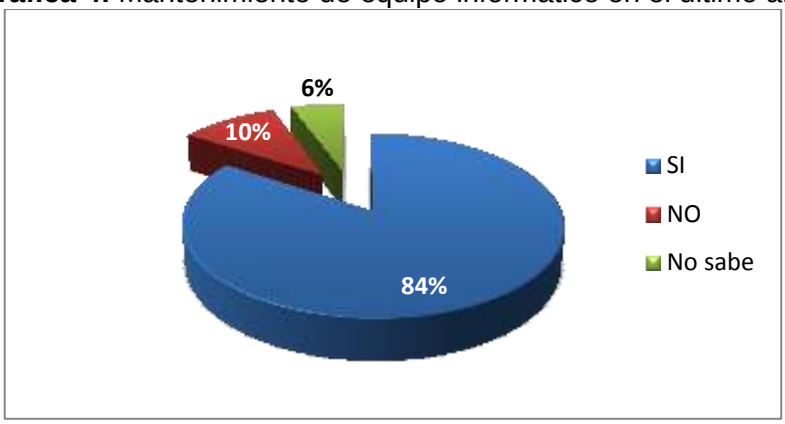
En el estudio realizado a las diversas instituciones se observó que aun cuando el 84% de las instituciones recibió mantenimiento en el último año, muchos de los usuarios afirmaron tener problemas con el equipo ya que este tenía demasiado tiempo de uso. El resultado se muestra en la gráfica siguiente:

Tabla 5: Mantenimiento del equipo

Mantenimiento	Instituciones	%
SI	91	84%
NO	11	10%
No sabe	6	6%

Fuente: Elaboración propia

Gráfica 4: Mantenimiento de equipo informático en el último año



Fuente: Elaboración propia

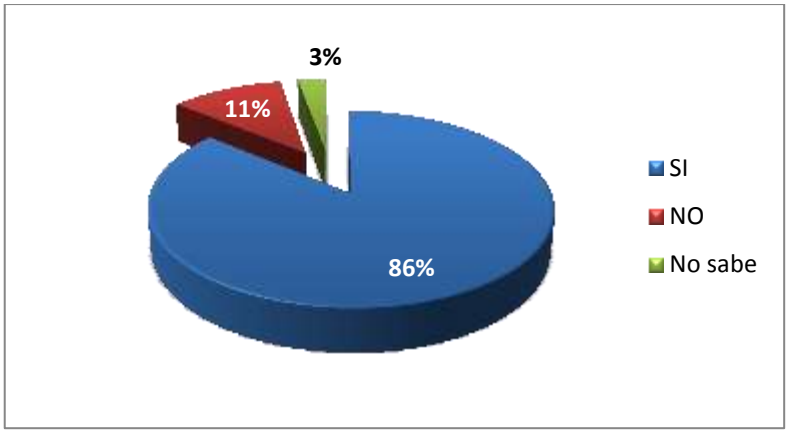
Un elemento importante que se analizó fue que el 86% de las instituciones confirmaron poseer un antivirus, pero cuando se les pregunto si este era efectivo en su mayoría los usuarios afirmaron que no, por estar demasiado desactualizado. Ver gráfica siguiente**:**

Tabla 6: Instituciones que poseen antivirus

Antivirus	Instituciones	%
SI	93	86%
NO	12	11%
No sabe	3	3%

Fuente: Elaboración propia

Gráfica 5: Instituciones que poseen antivirus



Fuente: Elaboración propia

- **Nivel de seguridad física**

La seguridad de la información puede estar amenazada por elementos físicos que pongan en riesgo las instalaciones y el equipo que resguarda la información por este motivo se tomó como un área principal para el estudio la seguridad física, considerando elementos como desastres naturales, mala ubicación del equipo, vulnerabilidad en el acceso a las instalaciones físicas entre otros elementos de vulnerabilidad que se identificaron en el departamento de San Vicente, para poder considerar dichos elementos se recurrió a investigaciones previas que analizaban las vulnerabilidades que presentaba el departamento, las investigaciones mencionadas están plasmadas en el documento denominado "Plan de Desarrollo del Departamento de San Vicente - TOMO II Diagnóstico del Departamento de San Vicente", en el cual se ha identificado vulnerabilidad y fragilidad ambiental referida a inundaciones, deslaves, sismos entre otros (Melara, 2004, p. 96).

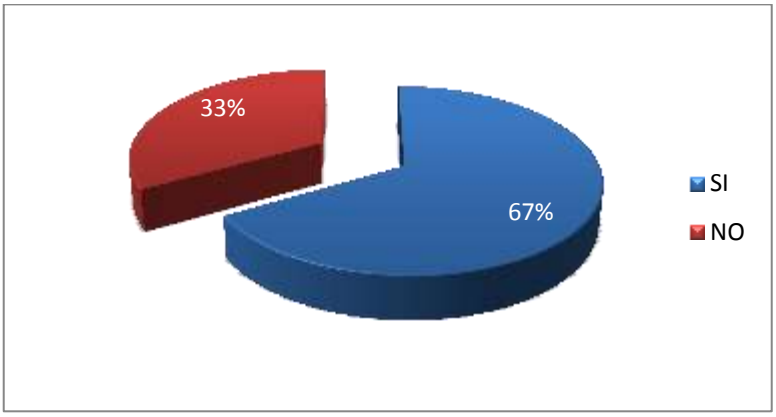
En la seguridad física además de la vulnerabilidad ambiental también se tomó en cuenta la ubicación del equipo que resguardaba la información ya que por medio del sondeo que se realizó con la encuesta denominada "Seguridad de la información" se identificó que una buena parte de las instituciones del departamento de San Vicente no contaban con el espacio suficiente para ubicar su equipo sin que pareciera saturado lo que podía conllevar a accidentes debido al reducido espacio con que se contaba. El resultado se muestra en la gráfica siguiente:

Tabla 7: Instituciones con espacio suficiente para ubicar el equipo

Espacio suficiente	Instituciones	%
SI	72	67%
NO	36	33%

Fuente: Elaboración propia

Gráfica 6: Espacio suficiente para ubicar todo el equipo sin que parezca saturado



Fuente: Elaboración propia

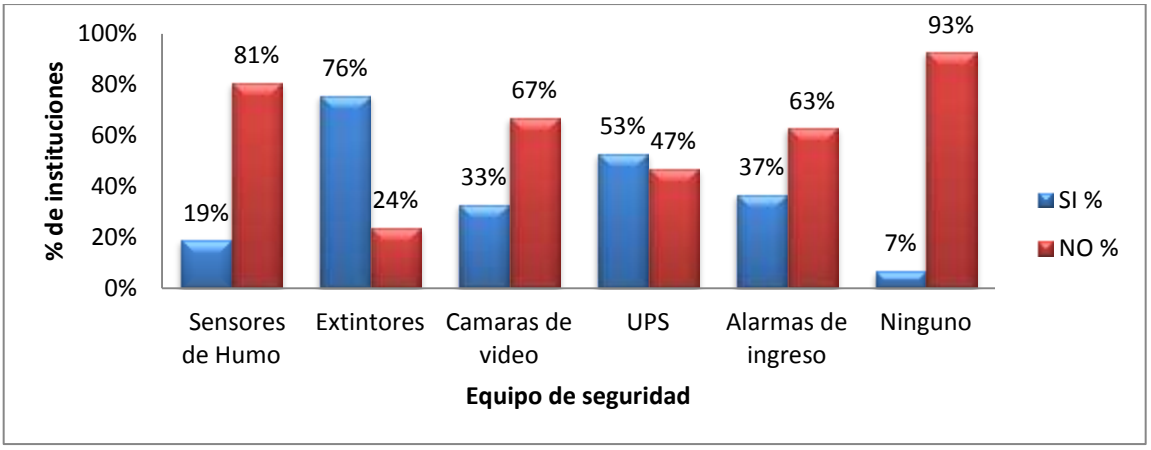
Otro elemento que se tomó como generador del problema de seguridad física fue la vulnerabilidad que presentaban las instalaciones ante accesos de personal no autorizado o delincuentes, debido a los altos índices de delincuencia del país y a los bajos mecanismos de seguridad con que contaban las instituciones, como también la falta de equipo de seguridad para la prevención ante desastres. El resultado se muestra en la gráfica siguiente:

Tabla 8: Equipo de seguridad con que cuentan las instituciones

Equipo de seguridad	SI	SI %	NO	NO %
Sensores de Humo	21	19%	87	81%
Extintores	82	76%	26	24%
Cámaras de video	36	33%	72	67%
UPS	57	53%	51	47%
Alarmas de ingreso	40	37%	68	63%
Ninguno	8	7%	100	93%

Fuente: Elaboración propia

Gráfica 7: Porcentaje de instituciones que poseen equipo de seguridad



Fuente: Elaboración propia

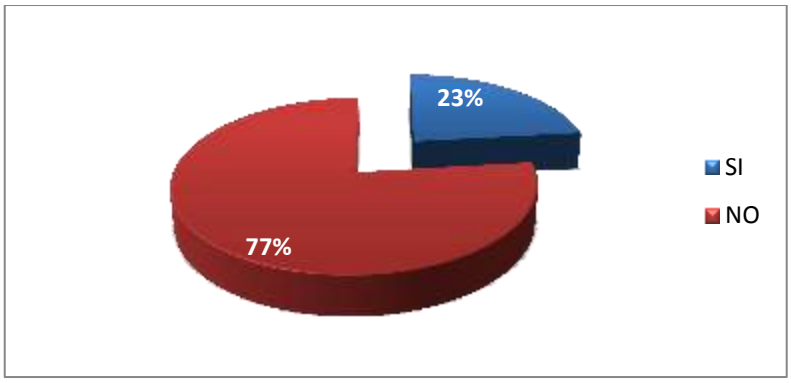
El equipo puede sufrir daños físicos por el derramamiento de sustancias o líquidos, esto se puede dar por el hecho de consumir alimentos o bebidas a una distancia muy cercana de los aparatos electrónicos, acción que no debería realizarse mientras se trabaja frente a ellos, pero las encuestas revelaron que los empleados estaban efectuando estas prácticas. El resultado se muestra en la gráfica siguiente:

Tabla 9: Consumo de alimentos mientras se trabaja en la computadora

Consume alimentos	Instituciones	%
SI	25	23%
NO	83	77%

Fuente: Elaboración propia

Gráfica 8: Consumo de alimentos mientras se trabaja en la computadora



Fuente: Elaboración propia

- **Nivel de seguridad en el manejo de información**

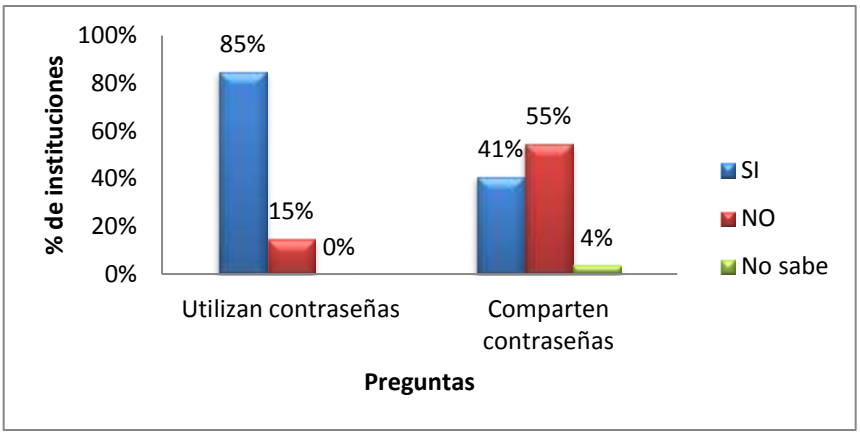
Se sabe que la información que las instituciones manejan es muy valiosa por lo que se debe proteger para que no sufra daños o sea utilizada para fines diferentes a los de la institución, según la información que se obtuvo por la población encuestada el 15% no poseía una contraseña para acceder a la información y de las que poseían un 41% la compartían. El resultado se muestra en la gráfica siguiente:

Tabla 10: Instituciones que hacen uso de contraseñas para acceder a la información

Se utiliza contraseña	Utilizan contraseñas	% que utilizan	Comparten contraseñas	% que comparten
SI	92	85%	38	41%
NO	16	15%	50	55%
No sabe	0	0%	4	4%

Fuente: Elaboración propia

Gráfica 9: Instituciones que hacen uso de contraseñas y las que la comparten



Fuente: Elaboración propia

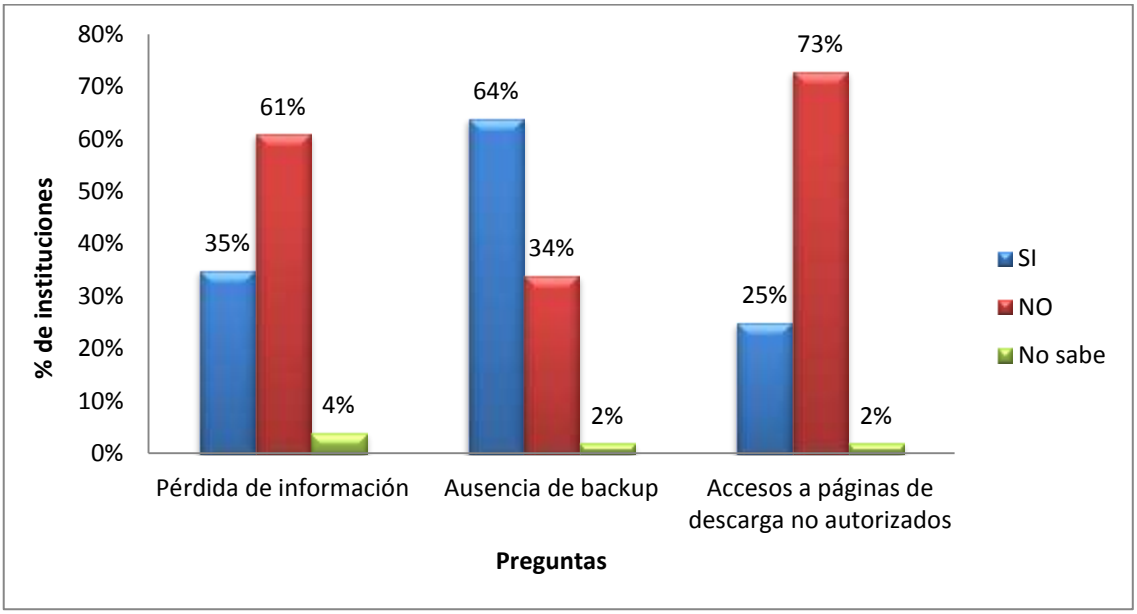
Se identificó que un 35% de los usuarios de los sistemas informáticos se habían enfrentado a pérdidas de información, este es un problema significativo ya que el 34% de los usuarios no realizaban copias de la información y un 25% accedían a páginas en internet no autorizadas exponiendo al equipo a contraer virus que pudieran dañar los programas utilizados para manejar la información. Estos factores entre otros se detallan más adelante en la descripción del diagrama causa-efecto. El resultado de este análisis se muestra en la gráfica siguiente:

Tabla 11: Instituciones que se han enfrentado a pérdidas de información

Se utiliza contraseña	Pérdida de información	%	Ausencia de backup	%	Accesos a páginas de descarga no autorizados	%
SI	38	35%	69	64%	27	25%
NO	66	61%	37	34%	79	73%
No sabe	4	4%	2	2%	2	2%

Fuente: Elaboración propia

Gráfica 10: Instituciones que han tenido problemas en el manejo de la información

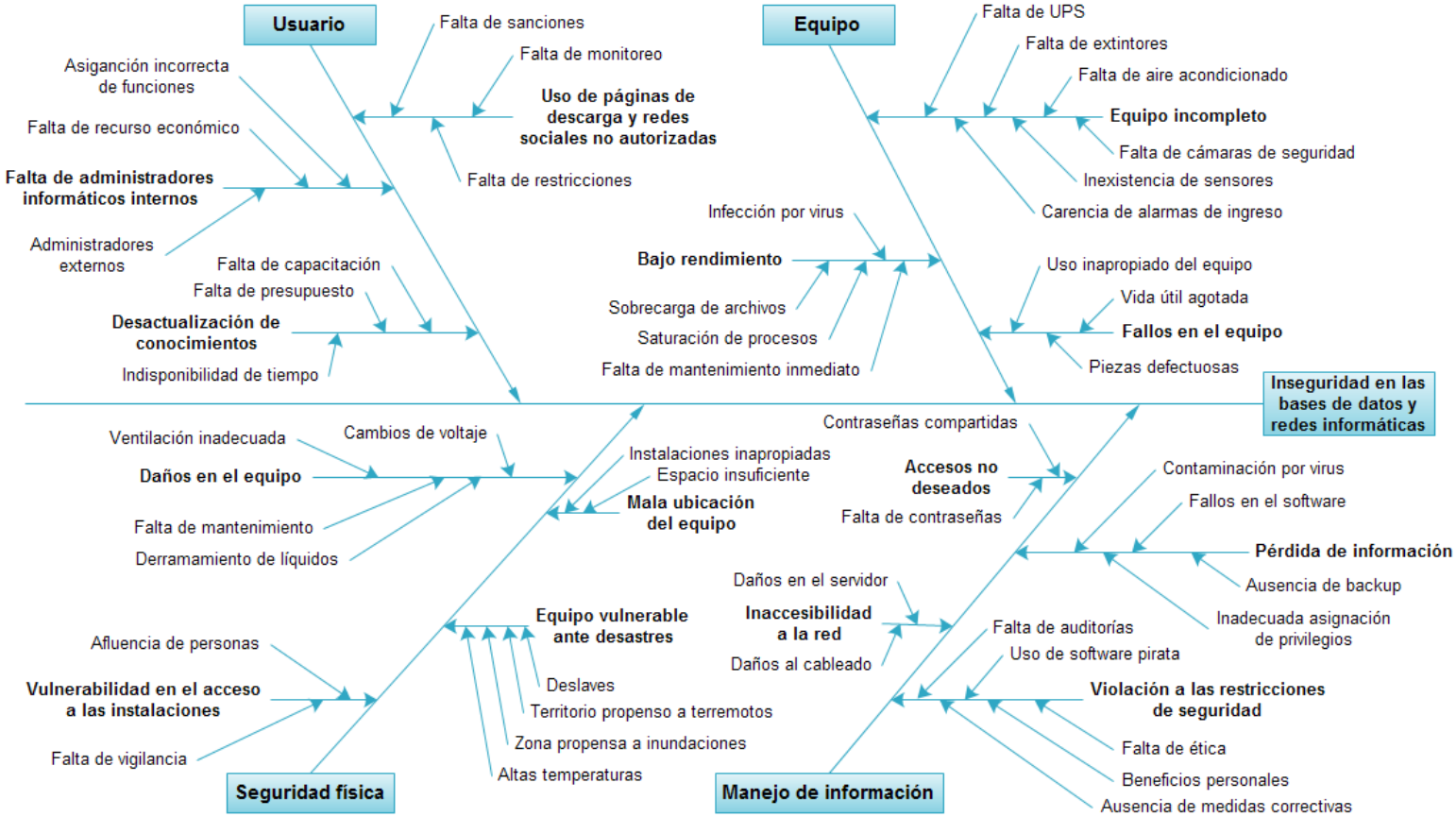


Fuente: Elaboración propia

Luego de haber analizado las áreas de mayor impacto para la problemática de la investigación, se determinó la problemática, utilizando el diagrama causa y efecto o espina de pescado.

1.1.2. Identificación del problema

Figura 1: Diagrama causa-efecto



Fuente: Elaboración propia

Descripción de las causas y sub-causas reflejadas en el diagrama causa-efecto

Tabla 12: Descripción de las causas del problema

CAUSA PRINCIPAL: USUARIOS El usuario es el responsable de manipular la información que se maneja en las empresas y organizaciones, ya sea usuario final o administrador está expuesto a cometer errores en el momento de realizar esta actividad por lo que pudo considerarse como una de las causas que originan el problema.
Sub –Causa: Falta de administradores informáticos internos En algunas de las instituciones el área informática era administrada desde oficinas centrales, otras contrataban personal ocasionalmente cuando surgía la necesidad o no poseían administrador informático. Agregando a esto que las instituciones tenían su sistema en red, y en caso que la red llegase a tener una falla tendrían que solicitar el mantenimiento a oficinas centrales por lo que se retrasarían algunos procesos. **Falta de recursos económicos** Toda organización busca minimizar recursos económicos y una alternativa es no asignar un salario fijo para el área de informática, se ha podido comprobar que la mayoría de instituciones no poseía recursos asignados específicamente para cubrir el área de informática. **Asignación incorrecta de funciones** Las funciones de administrador en algunos de los casos eran delegadas a empleados que cuentan con conocimientos básicos de computación pero que no está dentro de sus funciones desempeñar ese cargo. **Administradores externos** En las instituciones la administración externa a sustituido a la administración local, esto puede representar un problema ya que existen casos en los que se necesita la disponibilidad inmediata de una persona con conocimientos en el área y una administración externa implica en ocasiones tiempo de espera para la resolución de problemas.

Sub –Causa: Des-actualización de conocimientos

La falta de capacitación originaba estancamiento en cuanto a conocimiento de los administradores como también de los encargados del registro de información, razón por la cual la información se podía volver vulnerable, ya que la tecnología cambia con el paso del tiempo.

Falta de presupuesto

En muchas ocasiones las personas no se capacitan debido a que en sus instituciones no existe un fondo destinado a dichos fines, que les permita una adaptación a los cambios de tecnología.

Indisponibilidad de tiempo

Muchas personas no se actualizaban debido a que las instituciones no facilitaban tiempo de su jornadas laborales para darles la oportunidad a sus empleados de poder mejorar sus conocimientos, además las jornadas laborales cubrían en algunas ocasiones más de ocho horas diarias, agregando a esto la sobrecarga de trabajo que muchos poseían y las responsabilidades personales.

Falta de capacitación

La ausencia de capacitaciones periódicas llevaba a la desactualización del personal que manejaba información digital, ya que la tecnología evoluciona rápidamente y los conocimientos se van quedando obsoletos.

Sub –Causa: Uso de páginas de descarga y redes sociales no autorizadas

Por medio de estos accesos se podía contraer virus infectando las computadoras y dañando la información.

Falta de sanciones

Muchas personas accedían a estas páginas sin temor alguno, debido a que no existían medidas disciplinarias que sancionaran el uso de dichas páginas.

Falta de restricciones

Muchos administradores o encargados del área informática no usaban medios que permitieran controlar eficientemente el acceso a páginas de descarga redes sociales u otro tipo de accesos que pudieran causar daños a la información.

Falta de monitoreo

La falta de monitoreo constante por parte de la dirección permitía que los empleados llevaran a cabo acciones que en muchos de los casos se desconocían y que podrían tener efectos negativos para la institución.

CAUSA PRINCIPAL: EQUIPO

Las características y el estado del equipo utilizado para acomodar y acondicionar la instalación y resguardar los datos influían mucho en la seguridad de la información almacenada.

Sub-causa: Equipo incompleto

Las oficinas donde se alojaba el equipo informático de las instituciones públicas, privadas y no gubernamentales podían presentar falta de componentes básicos para mejorar la seguridad de los datos.

Falta de UPS

Algunas instituciones no poseían UPS, por lo tanto ponían en riesgo el equipo ante un cambio de voltaje y la información ante un corte eléctrico.

Falta de aire acondicionado

Pocas instituciones tenían aire acondicionado y otras poseían parcialmente, razón por la cual se exponía el equipo informático a un recalentamiento debido a las condiciones climáticas del departamento.

Carencia de alarmas de ingreso

Las instituciones no estaban equipadas con alarmas de ingreso pero contaban con equipo muy valioso, por lo que se encontraban más expuestas a robos debido a la delincuencia que enfrenta nuestro país El Salvador.

Inexistencia de sensores

Las instituciones no contaban con sensores de humo que les permitiera detectar a tiempo un caso de incendio y así evitar pérdidas totales.

Falta de cámaras de seguridad

Las instituciones no poseían cámaras de seguridad, por lo que no se podían hacer monitoreos en tiempo real para evitar accesos a personas no autorizadas o no se tenía evidencias en caso de que haya pérdidas de equipo o información.

Falta de extintores

Se identificó que las instituciones carecían de extintores, lo que podía poner en riesgo el equipo en caso de que fuera necesario detener un incendio.

Sub-causa: Bajo rendimiento

El bajo rendimiento del equipo electrónico e informático podía producir inconvenientes como: en el caso del aire acondicionado, podía producir sobrecalentamiento en las computadoras y en cuanto al equipo informático podría ocasionar congelamientos de pantallas, apagones y un lento rendimiento, por lo tanto si sucedían en momentos en que se procesaban los datos podían ocasionar inconsistencias y pérdida en estos.

Falta de mantenimiento inmediato

La falta de mantenimiento del equipo lograba producir inestabilidad que podría ocasionar inconvenientes en el momento de manipular los datos, las instituciones no contaban con personal encargado de dar mantenimiento al equipo, en caso que este fallará transcurría determinado tiempo antes de que el daño fuera reparado.

Saturación de procesos

Muchos de los equipos que poseían las instituciones podían producir un bajo rendimiento debido a que los empleados realizaban demasiadas actividades al mismo tiempo, excediendo así las capacidades del equipo.

Infección por virus

La contaminación por virus es un factor que afecta grandemente la eficiencia del equipo de las instituciones, ya que en muchos casos lo vuelve lento, oculta o destruye información valiosa, afecta el acceso a la red, inhabilitan el uso de programas, entre otros.

Sobrecarga de archivos

Las instituciones en algunos casos sobrecargaban sus equipos debido a que no poseían las capacidades necesarias para la cantidad de información que manejaban o en algunos casos los empleados excedían en el almacenamiento de archivos personales.

Sub-causa: Fallos en el equipo

Los fallos en el equipo podían ser generados por daños en el cableado, en las instalaciones eléctricas y/o porque el equipo llego a su máximo de vida útil, ocasionando inseguridad al momento de trabajar, lo que podía interrumpir procesos de edición de datos dejando incompleta la información.

Vida útil agotada

Durante la recolección de la información se pudo observar que en la mayoría de instituciones el equipo había sobrepasado su vida útil, este es un problema que exponía el manejo de la información ya que un equipo con mucho tiempo de uso está más expuesto a fallas.

Piezas defectuosas:

En muchos casos el equipo presenta fallos debido a que las piezas pueden estar dañadas, estos en ocasiones pueden ser superados por medio de un mantenimiento correctivo, en otros casos es necesario el reemplazo del equipo, lo que implica demora en el manejo de la información.

Uso inapropiado del equipo

En muchas ocasiones un mal uso del equipo puede provocar daños ya sea al equipo o a la información, entre los usos inapropiados identificados por medio de la recolección de información mencionamos el acceso a páginas de descargas personales, uso del equipo sin medios de protección, uso desproporcionado entre otros.

CAUSA PRINCIPAL: SEGURIDAD FÍSICA

La seguridad física es muy importante en una oficina o local donde se resguarda información importante ya que por descuidos en el entorno físico podrían producirse pérdidas muy significativas.

Sub-causa: Mala ubicación del equipo

La mala ubicación del equipo podía producir muchos accidentes y poner en riesgo al equipo que almacena y transporta los datos, este problema podía darse en muchos de los casos por no crear un diseño previo de la ubicación física del equipo, que permita reducir accidentes y maximizar la seguridad en casos de desastres como inundaciones, terremotos entre otros.

Espacio insuficiente

Se identificó que en las instituciones no había suficiente espacio para la ubicación del equipo por lo que volvía inapropiada para un uso cómodo.

Instalaciones inapropiadas

Según el estudio realizado las instalaciones físicas de instituciones y organizaciones del departamento de San Vicente en su mayoría no han sido diseñadas específicamente para ubicar el equipo y mobiliario de cada una de las entidades mencionadas, sino más bien se ha tratado de acomodar todo de la mejor manera en el espacio disponible.

Sub-causa: Daños en el equipo

El equipo está expuesto a sufrir daños que disminuyan el buen funcionamiento o que dañen permanentemente el equipo poniéndolo fuera de uso.

Ventilación inadecuada

Se identificó que las instituciones no poseían aire acondicionado parcial o totalmente, lo que podía provocar daños en el equipo informático producidos por el sobrecalentamiento, y de igual forma dañar piezas importantes del equipo.

Falta de mantenimiento

La falta de mantenimiento en el equipo informático o tecnológico podía producir daños debido a que la acumulación de partículas de polvo podía obstaculizar el buen funcionamiento de los componentes del equipo.

Cambios de voltaje

Los apagones repentinos provocados por la interrupción del suministro eléctrico podían producir cambios de voltaje provocando que los circuitos del equipo se quemen por las variaciones de la energía eléctrica.

Derramamiento de líquidos

Cuando no se cuenta con las restricciones necesarias con respecto al consumo de bebidas y alimentos frente a aparatos electrónicos se pueden provocar accidentes muy graves, con algo muy simple como es una taza de café; se podía producir un corto circuito que dañe muchos aparatos, poniendo en riesgo la información.

Sub-causa: Equipo vulnerable ante desastres

Las instalaciones que resguardan el equipo se construyen en ocasiones en lugares que son vulnerables a desastres lo que puede provocar daños cuantiosos, entre algunos de los desastres más comunes que fueron identificados en el departamento de San Vicente se pueden mencionar: Inundaciones, deslaves y terremotos.

Altas temperaturas

San Vicente por ser un departamento cercano a las costas del país tiende a tener temperaturas altas que facilitan la propagación de incendios y el sobrecalentamiento del equipo.

Territorio propenso a terremotos

Según el Consejo Departamental de Alcaldes de San Vicente en su estudio denominado Diagnóstico del Departamento de San Vicente TOMO II. catalogaban a San Vicente como un departamento con actividad sísmica debido a la presencia del volcán chinchontepec, lo que convierte al departamento en una zona más propensa a sismos y terremotos.(Melara y otros, 2004, p.98)

Deslaves

Según el Consejo Departamental de Alcaldes de San Vicente en su estudio denominado Diagnóstico del Departamento de San Vicente TOMO II. Los deslaves, lahares hacen vulnerables a las ciudades de San Vicente, Tepetitán, Guadalupe, San Cayetano Istepeque, Verapaz, Jerusalén, Mercedes La Ceiba y Tecoluca.(Melara y otros, 2004, p.100)

Zona propensa a inundaciones

Según el Consejo Departamental de Alcaldes de San Vicente en su estudio denominado Diagnóstico del Departamento de San Vicente TOMO II. Las inundaciones afectan a asentamientos ubicados en el Bajo Lempa, Distrito de Riego Lempa Acahuapa y aquellas ubicadas cerca de riberas de ríos. .(Melara y otros, 2004, p.100)

Sub-causa: Vulnerabilidad en el acceso a las instalaciones

La vulnerabilidad o la facilidad para poder ingresar a las instalaciones donde se tiene información importante convierte a los lugares que deberían ser privados en lugares con mucha afluencia de personas, esto aumenta la probabilidad de que se cometan actos que pasen desapercibidos y que pongan en riesgo la información.

Falta de vigilancia

La falta de vigilancia que existía en las instituciones en cuanto al acceso a las instalaciones las vuelve vulnerables ya que no se tiene un control apropiado si las personas que acceden a los locales en los que se maneja la información son personas autorizadas.

Afluencia de Personas

La afluencia de personas cerca del servidor y del equipo que resguardaba la información es otro factor que vulnerabiliza a las diferentes instituciones, ya que entre más personas asisten a un lugar más difícil se vuelve poder mantener el control apropiado.

CAUSA PRINCIPAL: MANEJO DE INFORMACIÓN

En el manejo de la información se debe considerar la accesibilidad a la información adecuada por personas apropiadas que puedan tener los privilegios correctos según el cargo o información que necesiten.

Sub-causa: Accesos no deseados

Que el sistema no estuviera protegido contra el acceso por parte de personas no autorizadas exponía la información a daños, hurtos y fraudes.

Falta de contraseñas

Se identificó que algunas instituciones no poseían una contraseña para el acceso a la información, por lo que se concluyó que algunos sistemas informáticos son vulnerables al robo de información.

Contraseñas Compartidas

Según el estudio realizado en las instituciones compartían la misma contraseña, esto representaba un problema de inseguridad ya que al manejarse información con una misma contraseña significaba responsabilidad compartida y en caso de que surgieran errores o incongruencia en la información iba ser difícil determinar al usuario responsable.

Sub-causa: Pérdida de información

La pérdida de información es un indicador que demostraba que se podían estar cometiendo errores en la forma de manipular la información o el equipo no tenía la capacidad y mantenimiento correcto para proporcionar la seguridad física adecuada para la información.

Fallos en el software

Si la calidad del software presentaba debilidades o imperfecciones tanto en su funcionalidad, fiabilidad, rendimiento, usabilidad, seguridad, entre otros, el software estaba propenso a sufrir fallos que a la larga se volvieran costosos y pudieran producir daños o pérdida de información.

Contaminación por virus

La contaminación por virus es una amenaza a la que cualquier institución pública o privada estaba expuesta, esta podía provocar daños leves o significativos en el software y en la información.

Ausencia de backup

La falta de generación de backup, ya sea en un sistema de forma automática o de forma manual, exponía a los datos a pérdidas irreparables en casos de desastres o daños repentinos del equipo**.**

Inadecuada asignación de privilegios

La inadecuada asignación de privilegios aumentaba la vulnerabilidad de la información ya que daba lugar a que usuarios no autorizados para tareas de escritura o eliminación pudieran realizar estas acciones por causa de una mala asignación de privilegios.

Sub-causa: Violación a las restricciones de seguridad

Esto podía afectar al manejo de la información ya que se volvía más vulnerable impidiendo alcanzar mayor desempeño en relación a las metas propuestas.

Falta de auditorías

Muchas personas se confiaban y tenían el hábito de violar las restricciones porque no existían auditorias constantes que verificaran el uso apropiado de los recursos de las instituciones.

Ausencia de medidas correctivas

Si no se contaba con medidas correctivas necesarias podía ocasionar problemas a la institución ya que los trabajadores podían cometer actos que dañaran la imagen de dicha institución o la información que manejaban y si estos actos no se corregían es probable que se siguieran dando.

Falta de ética

Este aspecto es muy importante ya que si un trabajador hace uso de medios inadecuados para acceder a la red estaría violando las medidas de seguridad establecidas por la institución, también la competencia desleal puede tentar a los trabajadores de la competencia a darles beneficios económicos u ofrecerles un mejor empleo en su empresa a cambio de que ellos les proporcionen información.

Beneficios personales

A veces los trabajadores infringen las reglas impuestas por las instituciones para obtener beneficios propios, los cuales pueden ser el dinero, un mejor puesto en otra empresa o la mala intención de perjudicar a la empresa ya que esta contiene información muy valiosa.

Uso de software pirata

El uso de software ilegal exponía en gran manera la información ya que muchos de ellos al instalarlos de forma ilegal, no solo se instala el programa sino también otros software espías.

Sub-Causa: Inaccesibilidad a la red

La falta de acceso a la red provoca un mal manejo de la información ya que en estos casos una de las alternativas de solución es realizar los procesos manualmente mientras se restaura la red, lo que aumenta las probabilidades de cometer errores al realizar procesos rezagados de ingreso de información al sistema.

Daños en el servidor

La disponibilidad inmediata de la información era una necesidad en la mayoría de instituciones en estudio, en algunas instituciones se observaban problemas en cuanto

al acceso a la información debido a que esta no estaba disponible en los servidores y que la mayoría de ellos eran administrados de manera externa.

Daños al cableado

Los daños causados en el cableado ya sea de la red externa de las instituciones o de los proveedores del servicio de internet podía provocar la inaccesibilidad de la información, lo que conllevaba a retrasos o pérdidas de los datos.

Fuente: Elaboración propia

1.1.3. Enunciado del problema

En base al análisis realizado anteriormente, se detalló el enunciado del problema en estudio:

"¿En qué medida la inseguridad de las bases de datos afecta la información manejada por las instituciones públicas, privadas y no gubernamentales del departamento de San Vicente?"

1.2. SISTEMA DE HIPÓTESIS

Definición de símbolos para hipótesis

Hg: Hipótesis general.
Ho: Hipótesis alternativa o nula.
H[n]: Hipótesis de trabajo.
Ho[n]: Hipótesis de trabajo alternativa o nula.
V.I: Variable independiente.
V.D: Variable dependiente.

1.2.1. Hipótesis General

Hg. En la Actualidad, las Instituciones públicas, privadas y no gubernamentales del departamento de San Vicente, no cuentan con una herramienta informática de evaluación que les permitan determinar el nivel de seguridad en sus bases de datos y redes informáticas.

Ho. En la Actualidad, las Instituciones públicas, privadas y no gubernamentales del departamento de San Vicente, cuentan con una herramienta informática de evaluación que les permitan determinar el nivel de seguridad en sus bases de datos y redes informáticas.

VI: Falta de herramienta informática de evaluación.

VD: Nivel de seguridad en sus bases de datos y redes informáticas

1.2.2. Hipótesis específicas de trabajo y nulas

Tabla 13: Hipótesis específicas de trabajo y nulas

HIPÓTESIS ESPECIFICAS O DE TRABAJO	HIPÓTESIS NULAS
H1. Actualmente los usuarios que laboran en las instituciones no están capacitados adecuadamente en aspectos de seguridad sobre la información que manejan.	**Ho1.** Actualmente los usuarios que laboran en las instituciones están capacitados adecuadamente en aspectos de seguridad sobre la información que manejan.
VI: Usuarios no capacitados **VD:** Poca seguridad sobre la información que manejan	
H2. La pérdida de información de las instituciones se debe a la falta de aplicación de medidas de seguridad lógica.	**Ho2**. La pérdida de información de las instituciones no se debe a la falta de aplicación de medidas de seguridad lógica.
VI: Falta de aplicación de medidas de seguridad lógica **VD:** Pérdida de información de las instituciones	
H3. Las instituciones no cuentan con un área informática interna que les brinde asistencia técnica inmediata.	**Ho3**. Las instituciones cuentan con un área informática interna que les brinde asistencia técnica inmediata.
VI: Falta de un área informática. **VD:** No se brinda asistencia técnica inmediata.	
H4. El equipo informático de las instituciones públicas, privadas y no gubernamentales se encuentra expuesto a riesgos físicos.	**Ho4**. El equipo informático de las instituciones públicas, privadas y no gubernamentales no se encuentra expuesto a riesgos físicos.
VI: Riesgos físicos. **VD:** Vulnerabilidad del equipo informático.	

Fuente: Elaboración propia

1.2.3. Operacionalización de hipótesis en variables

Tabla 14: Operacionalización de hipótesis en variables

HIPOTESIS	VARIABLES	INDICADORES
Hg. En la Actualidad, las Instituciones públicas, privadas y no gubernamentales del departamento de San Vicente, no cuentan con una herramienta informática de evaluación que les permitan determinar el nivel de seguridad en sus bases de datos y redes informáticas.	**VI:** Falta de herramienta informática de evaluación.	▪ Criterios de evaluación ▪ Conocimientos de seguridad informática
	VD: Nivel de seguridad en sus bases de datos y redes informáticas	▪ Estándares de seguridad utilizados ▪ Gestor de bases de datos utilizado ▪ Topología de red utilizada ▪ Herramientas de seguridad ▪ Métodos de accesos
H1. Actualmente los usuarios que laboran en las instituciones no están capacitados adecuadamente en aspectos de seguridad sobre la información que manejan.	**VI:** Usuarios no capacitados	▪ Grado académico ▪ Cargo ▪ Conocimientos de informática ▪ Disponibilidad de tiempo
	VD: Poca seguridad sobre la información que manejan.	▪ Políticas de seguridad implementadas ▪ Herramientas o equipo adecuado ▪ Tipo de información manejada ▪ Niveles de usuarios

H2. La pérdida de información de las instituciones se debe a la falta de aplicación de medidas de seguridad lógica.	**VI:** Falta de aplicación de medidas de seguridad lógica	◆ Falta de conocimiento ◆ Falta de recurso económico ◆ Políticas
	VD: Pérdida de información de las instituciones	◆ Protocolos utilizados ◆ Amenazas más comunes ◆ Copias de seguridad ◆ Antivirus
H3. Las instituciones no cuentan con un área informática interna que les brinde asistencia técnica inmediata.	**VI:** Falta de un área informática.	▪ Falta de recurso económico ▪ Conocimientos de seguridad informática ▪ Grado académico
	VD: No se brinda asistencia técnica inmediata.	▪ Equipo adecuado ▪ Personal no capacitado ▪ Accesibilidad
H4. El equipo informático de las instituciones públicas, privadas y no gubernamentales se encuentra expuesto a riesgos físicos.	**VI:** Riesgos físicos.	▪ Infraestructura ▪ Zona geográfica ▪ Clima ▪ Delincuencia
	VD: Vulnerabilidad del equipo informático.	▪ Vida útil ▪ Acondicionamiento ▪ Ubicación ▪ Capacidad

Fuente: Elaboración propia

1.3. DESCRIPCIÓN DEL TIPO, MÉTODO Y DISEÑO DE LA INVESTIGACIÓN

1.3.1. Tipo de estudio

La investigación que se realizó previamente para poder desarrollar el software dinámico para la evaluación de la seguridad de las bases de datos y redes informáticas en instituciones públicas, privadas y no gubernamentales del departamento de San Vicente fue de tipo:

Documental: Porque como investigadores nos apoyamos en los diversos documentos, tesis, bibliografías e investigaciones previas referidas al tema para tener una base de partida.

De campo: Ya que se obtuvo información proveniente entre otras, de entrevistas, encuestas y observaciones que se realizaron en la muestra de empresas e instituciones tomadas del departamento de San Vicente.

Descriptiva: Se describieron y analizaron los diferentes elementos que influyen en la seguridad de las bases de datos y redes informáticas.

1.3.2. Métodos y técnicas de investigación

Método utilizado en la investigación

En la investigación era preciso identificar el método que se utilizaría para poder alcanzar los objetivos propuestos, para ello se determinó como guía de la investigación al método científico.

El método científico tiene muchas clasificaciones por lo tanto debe identificarse de manera preliminar cual es la clasificación del método científico más adecuado para abordar la problemática en estudio, en nuestro caso después de haber analizado las clasificaciones del método científico concluimos que; para la investigación se utilizaría el **método hipotético-deductivo** porque es el que se fundamenta en la observación y en la experiencia que por sí misma proporciona hechos particulares, para concluir una verdad general; que es la que arrojara la realidad general de la seguridad de las bases de datos y redes informáticas en el departamento de San Vicente, esto por medio de la comprobación de hipótesis específicas.

Técnicas utilizadas en la investigación

La técnica es indispensable en el proceso de la investigación científica, ya que integra la estructura por medio de la cual se organiza la investigación, La técnica pretende los siguientes objetivos:

- Ordenar las etapas de la investigación
- Aportar instrumentos para manejar la información
- Llevar un control de los datos
- Orientar la obtención de conocimientos

En cuanto a las técnicas de investigación, se utilizaron dos formas generales: técnica documental y técnica de campo.

La técnica documental permite la recopilación de información para enunciar las teorías que sustentan el estudio de los fenómenos y procesos. Incluye el uso de instrumentos definidos según la fuente documental a que hacen referencia.

La técnica de campo permite la observación en contacto directo con el objeto de estudio, y el acopio de testimonios que permitan confrontar la teoría con la práctica en la búsqueda de la verdad objetiva.

Instrumentos de Investigación

Los instrumentos utilizados en cada una de las técnicas mencionadas anteriormente se describen a continuación:

- La investigación documental.
- La investigación de campo

Documental

La investigación de carácter documental se apoya en la recopilación de antecedentes a través de documentos tales como: guías, libros, revistas, publicaciones periódicas, tesis, manuales, entre otros; en donde servirá para fundamentar y completar la investigación con el aporte de diferentes autores, para ello existen los siguientes instrumentos.

- **Fichas de registro**

  Son los instrumentos de la investigación documental que permiten registrar los datos significativos de las fuentes consultadas. Las fichas bibliográficas y hemerográficas son las más comunes.

- **Fichas de investigación**

  Son las que permiten clasificar más fácilmente la información de acuerdo con el esquema de trabajo previamente diseñado entre algunos tipos de fichas de investigación se pueden mencionar: De resumen, cuadro sinóptico, textual o de transcripción.

- **Bitácoras de búsqueda:**

  Son formatos que permiten al investigador registrar los motores de búsqueda utilizados en internet. Permite tener un registro detallado de los sitios consultados, así como los hallazgos en dichas fuentes.

De campo

La investigación de campo se apoya en los instrumentos que se mencionan a continuación.

- **Entrevista:** Se utilizó para recabar información necesaria en base a puntos de vista de algunos administradores informáticos sobre la seguridad de la información en bases de datos y redes informáticas.

- **Encuesta:** Fue útil para recolectar datos sobre la seguridad de las bases de datos y redes informáticas, a partir de realizar un conjunto de preguntas dirigidas a la población en estudio.

- **Observación:** Fue útil para conocer los diferentes aspectos del problema, a fin de estudiar sus características y comportamiento dentro del medio en donde se desenvuelve éste.

1.3.3. Diseño de investigación

El diseño de la investigación fue orientado a instituciones públicas, privadas y no gubernamentales del departamento de San Vicente haciendo énfasis en los municipios que cuentan con mayor número de unidades económicas, siendo estos Apastepeque, Tecoluca, San Sebastián, y San Vicente. De dichas instituciones se tomó como población en estudio a las que registraban su información de forma digital ya sea por medio de sistemas, hojas de cálculo entre otros.

1.4. DETERMINACIÓN DEL UNIVERSO

1.4.1. Población

La población en nuestra investigación fue constituida por las instituciones públicas, empresas privadas y organizaciones no gubernamentales que registran su información de forma digital ya sea por medio de sistemas, hojas de cálculo entre otros, del departamento de San Vicente, específicamente de los municipios de Apastepeque, San Sebastián, San Vicente, y Tecoluca.

La población se detalla en la tabla siguiente.

Tabla 15: Población total

Municipios	Instituciones publicas	Empresas privadas	ONG's	Población Total
Apastepeque	6	1	-	7
San Sebastián	4	3	-	7
San Vicente	27	52	5	84
Tecoluca	5	3	2	10
Total población	42	59	7	**108**

Fuente: Elaboración propia

1.4.2. Cálculo de la muestra

Para el cálculo de nuestra muestra se consideró como población total 108 instituciones.

Fórmula para determinar el tamaño de la muestra conociendo la población:

$$n = \frac{k^2.p.q.m}{\left(e^2.(m-1)\right) + k^2.p.q}$$

m=tamaño de la población.
n=tamaño de la muestra
e=margen de error o precisión (5%)
k=desviación estándar (para margen de confianza de 95% es 1.96)
p=probabilidad de ocurrencia del suceso (cuando se desconoce se plantea un 50%)
q=1-p probabilidad de no ocurrencia (50%)

Cálculo de la muestra:

$$n=\frac{(1.96)^2*0.5*0.5*108}{\left((0.05)^2*(108-1)\right)+\ (1.96)^2*0.5.*0.5}$$

n≈ 84 Instituciones

1.4.3. Tipo de muestreo

Para realizar la selección de la muestra se optó por el muestreo aleatorio simple ya que es el que permite obtener una muestra donde todos los miembros de una población delimitada, tienen las mismas o por lo menos una característica para ser incluidos en ella.

1.5. PRESUPUESTO DEL PROYECTO

Fue necesario realizar una planificación de recursos para hacer una adecuada asignación de ellos en el proyecto, por lo que se detallan todos los recursos utilizados en la realización del mismo, Clasificándolos en: Recurso Humano, Recursos Materiales y Recursos Lógicos, para determinar el presupuesto estimado a cada uno de ellos los cuales vendrán a conformar el presupuesto total del proyecto. (Ver anexo Nº 9, Pág. 272).

Costos totales del proyecto

Se realizó un resumen de todos los costos incurridos para poder desarrollar el proyecto. Ver tabla siguiente.

Tabla 16: Costos totales del proyecto

Descripción	Sub Total Anual en ($)
Recurso Humano	13,200.00
Recursos Materiales	990.66
Software	600.00
Total	**14,790.66**

Fuente: Elaboración propia

Al total de los costos estimados se le agrego un porcentaje que correspondía a los imprevistos, como se muestra en la tabla siguiente.

Tabla 17: Costos con Imprevistos del proyecto

Descripción	Totales en ($)
Costos totales para el proyecto	14,790.66
Imprevistos (5%)	739.53
Costos Totales	**15,530.19**

Fuente: Elaboración propia

1.6. ESTUDIO DE FACTIBILIDADES

Se refiere a la disponibilidad de los recursos necesarios para llevar a cabo el proyecto, por lo que se tomó en cuenta las siguientes factibilidades:

- Técnica
- Operativa
- Económica Social

1.6.1. Factibilidad Técnica

Es la evaluación que demostró que el proyecto pudo desarrollarse por que se contaba con el conocimiento, técnicas, equipo y materiales para llevarlo a cabo.

Para el desarrollo de este proyecto de investigación se consideró que se tenían los conocimientos sobre investigación y sobre las técnicas necesarias para realizar el proceso de recolección, tabulación y análisis de la problemática, además se contaba las habilidades

para manipular herramientas y equipo informático que facilitarían el análisis de la información, ya que ha sido desarrollado por estudiantes egresadas de la carrera de ingeniería de sistemas informáticos.

Además se determinó por medio de un estudio preliminar que la población en estudio mostraba la disponibilidad de colaborar en el proyecto, brindándonos la información que se encontraba a su alcance.

También se disponía del equipo necesario para desarrollar tanto la investigación como el software, siendo este una impresora multifuncional, un modem y tres computadoras.

Por lo tanto pudimos concluir que el proyecto fue factible técnicamente, porque se pudo contar con los conocimientos, técnicas y el equipo necesarios para desarrollar satisfactoriamente el proyecto.

1.6.2. Factibilidad Operativa

Se refiere a que debía existir el personal capacitado requerido para llevar a cabo el proyecto y así mismo, debían existir usuarios finales dispuestos a emplear los productos o servicios generados por el proyecto o sistema desarrollado.

El software dinámico desarrollado está diseñado de tal forma que guie al usuario durante su uso para que pueda ser operado por personas que tengan únicamente conocimientos básicos de computación.

El software en conjunto con la investigación trae con ellos beneficios a instituciones, usuarios de la información, estudiantes y docentes.

Instituciones

- El software proporciona información sobre el nivel de seguridad con que se resguardan los datos, por medio de parámetros previamente establecidos y comparados con los utilizados por la institución.
- El software también brinda medidas preventivas y correctivas que ayuden a mejorar la seguridad lógica y física de bases de datos y redes informáticas.

- Con la investigación se brinda información actualizada sobre los riesgos lógicos y físicos más comunes en el departamento de San Vicente y cómo prevenirlos.

Usuarios de la información

- Se mejoraría la seguridad de los datos de los usuarios de las instituciones.
- Se fomentaría más la confianza por parte de los usuarios hacia las instituciones en las que se resguarda información valiosa.

Estudiantes

- Se proporcionó una base teórica sobre la seguridad de bases de datos y redes informáticas que permitan ser útiles para futuras investigaciones.
- Se proporcionó una perspectiva general de las instituciones del departamento de San Vicente que están trabajando con sistemas informáticos, brindando un panorama de la seguridad que estas presentan.
- Se brindaron los criterios de evaluación de la seguridad de las bases de datos y redes informáticas

Docentes

- Se dio a conocer una perspectiva general de la problemática sobre la seguridad de bases de datos y redes informáticas de las instituciones del departamento de San Vicente, para que los docentes puedan orientar las materias a fin a la realidad a que se enfrentan las instituciones actualmente.
- Se benefició a los docentes ya que se obtuvieron conocimientos actualizados para implementarlos en el proceso de enseñanza, y obtener un mejor desenvolvimiento laboralmente**.**

1.6.3. Factibilidad Económica Social

La factibilidad económica se refiere a la capacidad de obtener el capital en efectivo o los créditos financieros necesarios para invertir en el desarrollo del proyecto.

Debido a que nuestro proyecto es de carácter social no se consideró un análisis costo beneficio o un valor de recuperación cuantificado económicamente, ya que el proyecto no

presentó flujos de efectivo que sigan un patrón específico, dado que el software ha sido puesto a la disposición de diversas instituciones, con diferentes problemas de seguridad y las mejoras no se cuantifican económicamente porque no hay forma de identificar si las medidas de seguridad dadas por el software serán aplicadas. Como también dichas instituciones no necesitan hacer una inversión inicial para adquirir el software ya que es de carácter libre, por lo tanto se consideró únicamente los recursos económicos, materiales y lógicos necesarios para el desarrollo del proyecto, los cuales fueron financiados con fondos propios de las estudiantes desarrolladoras del proyecto. El proyecto fue económicamente factible ya que se contó con el capital y los recursos necesarios para asumir los gastos estimados.

CAPÍTULO II. FUNDAMENTOS TEÓRICOS DE LA INVESTIGACIÓN.

Síntesis

Es la etapa que incluye toda la temática necesaria para fundamentar los aspectos de seguridad de bases de datos y redes informáticas de la investigación esto se presenta por medio del marco teórico en el cual se consideran los elementos que influyen en la seguridad la cual se ha englobado de forma general en dos grandes áreas las cuales son seguridad física y seguridad lógica.

2.1. MARCO TEÓRICO

2.1.1. Seguridad en las bases de datos digitales

Seguridad física

Las bases de datos almacenan información extremadamente valiosa para las instituciones por lo tanto se debe trabajar constantemente en estrategias para protegerlas de las amenazas que aumentan los riesgos, para ello primeramente se deben conocer las vulnerabilidades que generan un punto susceptible para ser atacado o dañado, representando las debilidades o aspectos inseguros ante las amenazas.

Para lograr una mayor seguridad física en las bases de datos es preciso abordar por lo menos los puntos que se mencionan a continuación:

- **Vulnerabilidad de infraestructura.**

Se encuentra en el nivel del edificio o entorno físico de la información. Se relaciona con la posibilidad de entrar o acceder físicamente a la información para robar, modificar o destruir la misma, también se considera fallos eléctricos o picos de potencia y la mala ubicación del equipo.

- **Vulnerabilidad del hardware.**

Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del equipo que almacena la información fallen ya sea por mal uso, descuido, mal diseño, dejando la información desprotegida o inaccesible.

- **Vulnerabilidad de los medios o dispositivos de almacenamiento de la información.**

Se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresoras o cualquier otro medio de respaldo de la información.

- **Vulnerabilidad por errores humanos.**

La gente que administra y utiliza la información representa la mayor vulnerabilidad de la información. Toda la seguridad de la información descansa sobre el administrador del mismo que tiene acceso al máximo nivel y sin restricciones al mismo.

Los usuarios de la información. También suponen un gran riesgo al mismo. Ellos son los que pueden acceder al mismo, tanto físicamente como mediante conexión.

Por todo ello hay una clara diferenciación en los niveles de los distintos tipos de vulnerabilidad y en las medidas a adoptar para protegerse de ellos.

2.1.2. Guía para alcanzar los requerimientos proactivos de seguridad en las bases de datos

Como una guía para que las instituciones puedan alcanzar los requerimientos proactivos de seguridad se proporcionan las siete fases planteadas por Slemo Warigon.

Las fases establecidas por Slemo Warigon son las siguientes:

1. Identificar los datos
2. Clasificar los datos
3. Cuantificar el valor de los datos
4. Identificar las vulnerabilidades de seguridad de los datos
5. Identificar las medidas de protección de los datos y su costo
6. Seleccionar las medidas de seguridad que resulten favorables en la relación costo-beneficio
7. Evaluar la efectividad de las medidas de seguridad

A continuación se describen cada una de las fases.

1. Identificar los datos

Se deben identificar todos los datos almacenados digitalmente dentro de la empresa que están puestos en el depósito de datos. Esta es una situación que frecuentemente se ignora, pero que se vuelve crítica para reunir los requerimientos de seguridad de un ambiente de depósito de datos desde sus inicios y hacia las etapas subsecuentes.

2. Clasificar los datos

La clasificación de todos los datos contenidos en un ambiente de depósito de datos es necesaria para satisfacer, de una manera prudente, los requerimientos de confidencialidad, integridad y disponibilidad de los datos. Los datos se clasifican generalmente sobre la base de la criticidad o sensitividad ante la exposición indebida, modificación o destrucción. La sensitividad de los datos de una empresa se puede clasificar en:

Públicos (los datos menos sensitivos): los datos de esta categoría usualmente no se clasifican y están propensos a la exposición pública por leyes, prácticas comerciales comunes, o políticas de la compañía. Todos los niveles de usuarios finales del depósito de datos pueden tener acceso a ellos.

Confidenciales (datos moderadamente sensitivos): los datos de esta categoría no están sujetos a la exposición pública. Para la clasificación de los datos de esta categoría se aplica el principio del mínimo privilegio, los usuarios sólo pueden tener acceso a estos datos si éstos son necesarios para realizar exitosamente su trabajo.

Muy confidenciales (los datos más sensitivos): los datos de esta categoría son altamente sensitivos y de misión crítica. El principio del mínimo privilegio también aplica a esta categoría (con requerimientos de acceso mucho más exigentes que para los datos confidenciales). Sólo los usuarios del más alto nivel del depósito de datos (es decir, con acceso ilimitado), con los permisos de seguridad apropiados pueden accesarlos.

3. Cuantificar el valor de los datos

El proceso de cuantificación trata principalmente de asignar un valor real de los datos agrupados en las diferentes categorías de sensitividad. Por sí mismo, los datos no tienen un valor intrínseco. Sin embargo, el valor definitivo de los datos es frecuentemente medido por el costo de:

a) Reconstruir datos perdidos

b) Restaurar la integridad de datos corruptos, interceptados o fabricados

c) No tomar a tiempo una decisión a causa de la falta de servicio, o

d) Pagar obligaciones financieras por la exposición pública de datos confidenciales.

El valor de los datos puede incluir ingresos dejados de recibir por causa de la fuga de secretos empresariales hacia sus competidores, y el uso anticipado de datos financieros secretos por parte de empleados deshonestos, antes de que éstos se hagan públicos en el mercado.

4. Identificar las vulnerabilidades de seguridad de los datos

Esta fase requiere la identificación y documentación de las vulnerabilidades asociadas al ambiente de depósito de datos. Algunas de las vulnerabilidades de los depósitos de datos más comunes incluyen las siguientes:

Amenazas internas: los usuarios (empleados) representan la más grande amenaza contra los datos valiosos. Empleados disgustados con acceso legítimo podrían revelar datos secretos a las empresas competidoras y divulgar públicamente ciertos datos confidenciales del recurso humano de la empresa. Empleados deshonestos podrían también obtener un beneficio personal al utilizar datos estratégicos de la empresa antes de que ésta se haga pública en el mercado.

Amenazas externas: Incluyen espionaje electrónico y otras técnicas similares para robar, comprar o reunir datos estratégicos en un ambiente de depósito de datos. La pérdida resultante tiende a ser mucho más alta que la provocada por ataques internos.

Factores naturales: Daños provocados por el fuego, el agua y el aire pueden hacer que tanto los servidores como los clientes de un ambiente de depósito de datos se vuelvan inutilizables. Los riesgos y pérdidas varían de organización en organización, dependiendo mayormente de la ubicación y los factores de contingencia.

Factores de utilidad: La interrupción del fluido eléctrico y del servicio de comunicaciones pueden causar costos disturbios en un ambiente de depósito de datos. Estos factores tienen una muy baja probabilidad de ocurrencia, pero tienden a causar pérdidas cuantiosas.

5. Identificar las medidas de protección de los datos y su costo

Las vulnerabilidades identificadas en la fase anterior deben ser consideradas en la medida de determinar las protecciones que resulten favorables en la relación costo-beneficio para los datos del depósito de datos a diferentes niveles de sensitividad. Algunas medidas de protección para los datos en el depósito incluyen:

La barrera humana: los empleados representan el frente de defensa contra las vulnerabilidades de seguridad en cualquier ambiente de procesamiento centralizado, incluidos los depósitos de datos. Enfocarse en la contratación y entrenamiento del personal (sobre todo en lo que respecta a la conciencia de la seguridad). Este método efectivamente ataca los orígenes, más que los síntomas de los problemas de seguridad.

Encriptación de datos: se deben cifrar los datos sensitivos del depósito para asegurar que éstos sólo sean accesados por las personas autorizadas. Ello anula el valor potencial de los datos interceptados, así como la fabricación o modificación de éstos.

Controles de acceso: se deben utilizar políticas de control de acceso basadas en los principios del mínimo privilegio y la protección adecuada de los datos. Se deben establecer restricciones de los controles de accesos efectivos y eficientes de modo que los usuarios finales puedan accesar sólo los datos y programas para los cuales ellos tienen los legítimos privilegios.

6. **Seleccionar las medidas de seguridad que resulten favorables en la relación costo-beneficio**

Todas las medidas de seguridad implican gastos, y los gastos en seguridad requieren justificación. Esta fase descansa en los resultados de las fases anteriores para valorar el impacto fiscal de los datos corporativos en riesgo, y seleccionar las medidas que resulten favorables en su relación costo-beneficio para salvaguardar los datos contra vulnerabilidades conocidas. Seleccionar medidas de seguridad que resulten favorables en su relación costo-beneficio es congruente con una práctica del negocio prudente la cual asegure que los costos de protección de los datos en riesgo no excedan la pérdida esperada máxima para los datos.

7. **Evaluar la efectividad de las medidas de seguridad**

Para evaluar la efectividad de las medidas de seguridad se deben dirigir los esfuerzos para determinar continuamente si las medidas son:

- Pequeñas, simples y directas.
- Analizadas, probadas y verificadas cuidadosamente.
- Utilizadas y seleccionadas apropiadamente de modo que no excluyan los accesos legítimos.
- Elásticas de modo que puedan responder efectivamente a cambios en los requerimientos de seguridad.

- Razonablemente eficientes en términos de tiempo, espacio de memoria, y actividades centradas en el usuario, de modo que no afecten adversamente a los recursos computacionales protegidos.

Es igualmente importante asegurar que los usuarios finales del depósito de datos entiendan y adopten la responsabilidad de las medidas de seguridad a través de un programa de concienciación de seguridad efectivo. El administrador del depósito de datos con la autoridad delegada por la administración superior es el responsable por asegurar la efectividad de las medidas de seguridad (Gámez, 2002, pp.142-150).

2.1.3. Elección del sistema gestor de bases de datos

Antes de profundizar en los elementos que deben considerarse para la elección del sistema gestor de bases de datos veremos las ventajas que trae su utilización

Ventajas de los sistemas gestores de bases de datos (SGBD)

Con la implementación de sistemas gestores de base de datos podemos obtener las siguientes ventajas en comparación con los sistemas de archivos:

- Consultas no predefinidas y complejas

Los SGBD permiten que se hagan consultas no predefinidas y complejas. Los usuarios pueden hacer consultas creando filtros para la información requerida y procesos para extraer datos que proporciones mayor información

- Disminuye problemas de la redundancia

La duplicación de datos es el tipo de redundancia más habitual, así pues, el verdadero problema es el grave riesgo de inconsistencia o incoherencia de los datos; si tenemos algo apuntado en dos lugares diferentes no pasará demasiado tiempo hasta que las dos anotaciones dejen de ser coherentes, porque habremos modificado la anotación en uno de los lugares y nos habremos olvidado de hacerlo en el otro. Este riesgo se reduce con la utilización de SGBD y la aplicación de bases de datos bien diseñadas.

- Aumenta la integridad de los datos

El SGBD puede llevar el control de las actualizaciones en el caso de las redundancias, para garantizar la integridad. Del mismo modo, podremos darle otras reglas de integridad –o restricciones– para que asegure que los programas las cumplen cuando efectúan las actualizaciones.

- Mayor seguridad

Los SGBD permiten definir autorizaciones o derechos de acceso a diferentes niveles: al nivel global de toda la BD, al nivel entidad y al nivel atributo. Estos mecanismos de seguridad requieren que el usuario se pueda identificar (Campos, 2005, pp.15-21).

Proceso de selección de un SGBD

Según Gints Plivna analista de sistemas en Rix Technologies existen "criterios generales a considerar al momento de seleccionar, implementar y analizar la seguridad de un gestor de bases de datos".

Entre los cuales tenemos los siguientes:

Todas las bases de datos son diferentes

Cada base de datos es particular, todas tienen diferentes arquitecturas y no puede aplicárseles las mismas prácticas de manera específica.

Entender los requerimientos actuales pero planear los requerimientos a futuro

Este es el criterio principal, deben entenderse los requerimientos funcionales y no funcionales para escoger el SGBD de la base de datos que mejor se ajuste a estos requerimientos.

Los requerimientos deberían de ser al menos los siguientes:

1. Cantidad de datos y tipo de datos (texto, binarios, espacial u otros tipos específicos)
2. Número simultaneo de usuarios (concurrencia a la base de datos)
3. Disponibilidad: Cuanto tiempo puede permitir tener de baja su base de datos.

4. Escalabilidad: qué hará cuando la cantidad de datos y el número de usuarios aumente.
5. Seguridad: cuanto necesitará de características como seguridad y encriptación de datos, administración de usuarios, privilegios.
6. Manejo y administración: cuan amigable quiere que sea la administración de su base de datos.

Es razonable elaborar los requerimientos en función de sus recursos y necesidades reales. Pero es recomendable ver un poco hacia el futuro y modificar los requerimientos acorde al mismo.

Situación actual, analizar si el SGBD debe cooperar con un sistema existente o es el primero en ser implementado.

Hay una gran diferencia si un proyecto es el primero en determinada área o si debe considerar a otros sistemas con los que debe colaborar. En el primer caso se tiene mucha mayor libertad. En el segundo caso, debe lidiar con el hecho que usualmente las bases de datos se integran más fácilmente con bases de datos del mismo fabricante que las de la empresa rival.

Evaluar la oferta laboral

Es importante asegurarse de que se podrá encontrar a una persona experta en caso de que la base datos falle. Aunque sea su empleado o un especialista de una empresa consultora, debe haber al menos una persona más a quien se confíe la administración de la bases de datos. Es muy desagradable pagar mucho porque un día alguien tenga que restaurar la base de datos pero es mucho más desagradable darse cuenta de que no hay nadie que lo pueda hacer.

Licencias

El costo de la licencia es tan solo uno de los factores que influyen en el costo directo, sin mencionar de costos indirectos asociados a determinada base de datos.

Soporte

Investigar cuánto cuesta el soporte, y que ofrece ese soporte. Usualmente existen muchos niveles con diferentes características y precios.

Características adicionales

Algunas SGBD contienen características adicionales más allá de "la versión empresarial", por un precio adicional. Si realmente no se necesitan esas características se puede solicitar descuentos adiciónales.

Requisitos del sistema operativo

Algunas bases de datos requieren sistemas operativos específicos. Los sistemas operativos como los SGBD son diferentes, requieren diferentes tipos de administración y de habilidades.

Hardware necesario

Es necesario conocer que plataformas de hardware requiere el SGBD y cuáles son los parámetros mínimos. Por supuesto que depende de la cantidad de datos esperada, de la cantidad de usuarios y la carga esperada en general.

2.1.4. Seguridad en las redes informáticas

La seguridad informática consiste en una estrategia de disminución del riesgo. En el caso de la seguridad en la red, busca mantener la integridad, disponibilidad y confidencialidad de la información dentro de la red, para que la institución mantenga la continuidad en sus procesos.

Cuando hablamos de integridad queremos decir que la información sólo puede ser modificada por personas autorizadas y en forma controlada. Por otro lado disponibilidad significa que la información de las bases de datos debe estar accesible a las personas autorizadas siempre que sea necesario. Por último, podemos definir confidencialidad en el sistema cuando la información contenida en el mismo no es brindada hacia entidades externas.

Para lograr un nivel de seguridad lógica de las redes informáticas que disminuyan los riesgos se han retomado los objetivos siguientes planteados en la monografía “Seguridad en redes”, presentada por el Instituto de Ciencias Básicas e Ingeniería.

1. Restringir el acceso a los programas y archivos

2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

3. Asegurar que se estén utilizando los archivos y programas con el procedimiento correcto

4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.

5. Que la información recibida sea la misma que ha sido transmitida.

6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

(Sánchez, (s. f.), p. 7)

2.1.5. Barreras y procedimientos que resguarden el acceso a los datos

a) Controles de acceso

Estos pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario. Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados. Así mismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

El National Institute for Standars and Technology (NIST) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

- Identificación y autenticación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina **identificación** al momento en que el usuario se da a conocer en el sistema; y **autenticación** a la verificación que realiza el sistema sobre esta identificación.

- Limitación a los servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema

- Modalidad de acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

Lectura: el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.

Escritura.: este tipo de acceso permite agregar datos, modificar o borrar información.

Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas.

Borrado: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.

Creación: permite al usuario crear nuevos archivos, registros o campos.

Búsqueda: permite listar los archivos de un directorio determinado

b) Control de acceso interno

- Palabras clave. (passwords)

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras claves resultan de muy bajo costo, sin embargo, cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas, encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Sincronización de passwords: Consiste en permitir que un usuario acceda con el mismo password a diferentes sistemas interrelacionados y a su actualización automática en todos ellos en caso de ser modificada.

Caducidad y control: este mecanismo controla cuando pueden y/o deben cambiar sus passwords los usuarios. Se define el periodo mínimo que debe pasar, para que los usuarios puedan cambiar sus passwords y un periodo máximo que puede transcurrir para que éstos caduquen.

- Encriptación

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

- Listas de control de accesos

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

- Limites sobre la interface de usuario

Estos límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interface de usuario.

- Etiquetas o políticas de seguridad

Consiste en designaciones otorgadas a los recursos, pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc., estas etiquetas no son modificables.

c) Control de acceso externo

- Dispositivos de control de puertos

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar fácilmente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un MODEM.

- Firewall o puertas de seguridad

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Este tema será abordado posteriormente.

- Acceso de personal contratado o consultores

Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.
(Sanchez,(s. f.), p. 8-15)

CAPÍTULO III. RECOLECCIÓN, PRESENTACIÓN Y ANÁLISIS DE LA INFORMACIÓN.

Síntesis

En este capítulo se da a conocer el área geográfica tomada para el estudio y el desarrollo del proyecto, además se presentan los instrumentos utilizados para la recopilación de la información, los cuales permitirán conocer el nivel de seguridad física y lógica de las bases de datos y redes informáticas de las entidades evaluadas, para finalizar el capítulo se presenta el análisis de cada una de las hipótesis planteadas en la investigación.

3.1. Delimitación del área geográfica

El área geográfica que se estableció para la investigación está delimitada por los cuatro municipios con mayores unidades económicas del departamento de San Vicente siendo estos: Apastepeque, Tecoluca, San Sebastián y San Vicente, eligiendo de estos una muestra de 84 instituciones entre estas públicas, privadas y ONGs (ver anexo Nº 2, pág. 230), las cuales se encuentran distribuidas de la siguiente manera:

Tabla 18: Población

Institución	Población
San Vicente	62
San Sebastián	6
Apastepeque	7
Tecoluca	9
Total	**84**

Fuente: Elaboración propia

3.1.1. Encuesta sobre seguridad de la información

Encuesta dirigida a instituciones

Para la investigación se diseñó un instrumento de recolección de información que permitió indagar sobre los aspectos de seguridad de las instituciones públicas, privadas y no gubernamentales del departamento de San Vicente. El instrumento que fue denominado "Encuesta sobre seguridad de la información" (anexo 3, pág. 246). El objetivo de dicho instrumento era el obtener información sobre los niveles de seguridad en las bases de datos y redes informáticas de instituciones públicas, empresas privadas y organizaciones no gubernamentales del departamento de San Vicente, lo que nos permitió aceptar o rechazar las hipótesis planteadas para la investigación por medio de las preguntas diseñadas, que están relacionadas con los indicadores correspondientes a las variables de las hipótesis.

3.1.2. Cuadro resumen de resultados

A continuación se muestra un cuadro con el resumen de los resultados obtenidos con la encuesta realizada a las 84 instituciones del departamento de San Vicente sobre seguridad informática.

Tabla 19: Cuadro de resumen de los resultados obtenidos

Pregunta	Opciones	Resultado
1-¿En su lugar de trabajo cuentan con un departamento de informática interno?	Si	10.71%
	No	89.29%
	No sabe	0%
2-¿En su lugar de trabajo se cuenta con los recursos económicos para la compra de equipo informático?	Si	29.76%
	No	65.48%
	No sabe	4.76%
3-¿La asistencia técnica al equipo informático de su lugar de trabajo es proporcionada por?	Técnicos de sede central	46.43%
	Técnicos locales	11.90%
	Técnicos por contrato temporal	28.57%
	No recibo asistencia	4.76%
	No sabe	8.33%
4-¿En su lugar de trabajo poseen herramientas para realizar el mantenimiento del equipo informático?	Si	15.48%
	No	80.95%
	No sabe	3.57%

5-¿En caso de fallos en el equipo y/o en la red en cuanto tiempo aproximadamente recibe asistencia técnica?	Inmediatamente	29.76%
	De 1 a 5 días	51.19%
	De 6 a 15 días	4.76%
	De 16 a 30 días	4.76%
	Más de 30 días	0
	No recibo asistencia	7.14%
	No sabe	2.38%
6 - ¿En su lugar de trabajo se ha invertido presupuesto en los últimos dos años en la compra de programas informáticos actualizados?	Si	45.24%
	No	46.43%
	No sabe	8.33%
7 - ¿En su lugar de trabajo le evalúan la seguridad con que maneja la información almacenada digitalmente?	Si	33.33%
	No	64.29%
	No sabe	2.38%
8 - ¿Conoce algún programa para evaluar el nivel de seguridad con que se maneja la información digital?	Si	2.38%
	No	97.62%
9 - ¿Cuentan localmente con un programa que les permita evaluar la seguridad de las bases de datos y redes informáticas? (no se consideran los antivirus)	Si	2.38%
	No	91.67%
	No sabe	5.95%

10 - ¿En el último año se ha invertido presupuesto en aspectos que contribuyan en la mejora de la seguridad de la información perteneciente a la institución donde labora?	Si	26.19%
	No	59.52%
	No sabe	14.29%
11-¿En su lugar de trabajo se asigna periódicamente parte del tiempo laboral, a capacitaciones sobre seguridad informática?	Si	22.62%
	No	75.00%
	No sabe	2.38%
12-¿Cada cuánto tiempo recibe cursos de actualización sobre seguridad informática?	Mensual	0
	Semestral	7.14%
	Anual	15.48%
	No recibe	77.38%
13-¿Cuál de las siguientes afirmaciones describe mejor la condición de las políticas de seguridad informática en su lugar de trabajo?	No se tienen políticas de seguridad definidas	60.71%
	Actualmente se encuentran en desarrollo	14.29%
	Política formal, no implementada	7.14%
	Política formal, escrita documentada e informada a todo el personal	9.52%
	No sabe	8.33%

14-¿Hace uso de las siguientes herramientas en su equipo de trabajo?	Skype	30.95%
	Atube Catcher	8.33%
	Ares	8.33%
	Emule	1.19%
	Ninguno	57.14%
	Otros	7.14%
15-Cuándo se realizan actualizaciones en el sistema informático ¿Se imparten las capacitaciones necesarias?	Si	34.52%
	No	60.71%
	No sabe	4.76%
16-La información que maneja en su lugar de trabajo es de carácter: (selección múltiple)	Publico	8.33%
	Privado	72.62%
	Ambos	19.05%
17-¿Utiliza contraseña para acceder a la información que almacena en su equipo de trabajo?	Si	80.95%
	No	19.05%
18¿Cada cuánto tiempo cambia la contraseña de acceso a los datos que maneja en su lugar de trabajo?	Quincenal	2.38%
	Mensual	15.48%
	Semestral	13.10%
	Anual	15.48%
	Nunca	34.52%
	No utilizo contraseña	19.05%

19-¿Se ha enfrentado a alguna de las siguientes amenazas de seguridad de la información? (selección múltiple)	Virus	78.57%
	Hurto de contraseñas	3.57%
	Intrusos informáticos	5.95%
	Alteración de los datos	9.52%
	Robo de información	2.38%
	No sabe	3.57%
	Ninguno	13.10%
	otros	2.38%
20-¿Cuáles de los siguientes medios utiliza actualmente la institución para almacenar las copias de seguridad?	Respaldo en discos duros	69.05%
	Respaldos en CD	22.62%
	Respaldos en USB	53.57%
	No sabe	1.19%
	Ninguno	5.95%
	Otros	2.38%
21-¿Se almacena alguna copia de seguridad fuera de los locales de trabajo?	Si	23.81%
	No	67.86%
	No sabe	8.33%
22-La versión del antivirus utilizado en su lugar de trabajo es	Gratuita	38.10%
	Pagada	40.48%
	No sabe	17.86%
	No se cuente con antivirus	3.57%

23-¿Seleccione los problemas de infraestructura que representan riesgo para los equipos que almacenan la información en su lugar de trabajo?	Mala ubicación de tomacorrientes	17.86%
	Tomacorrientes insuficientes	27.38%
	Ventilación inapropiada	45.24%
	Infiltración de agua	14.29%
	Poco espacio	27.38%
	No sabe	5.95%
	Ninguno	23.81%
24-¿El equipo Informático en que trabaja ha presentado problemas de sobrecalentamiento?	Si	36.90%
	No	58.33%
	No sabe	4.76%
25-¿En su lugar de trabajo se han presentado casos de robo de equipo informático?	Si	9.52%
	No	86.90%
	No sabe	3.57%
26-¿Aproximadamente cuánto tiempo tiene de uso la computadora en que trabaja?	Menos de 1 año	14.29%
	De 1 a 2 años	25.00%
	De 3 a 5 años	33.33%
	Más de 5 años	27.38%

27-¿En su lugar de trabajo cuentan con alguno de los siguientes tipos de red? (Selección múltiple).	Red cableado	60.71%
	Red inalámbrica	58.33%
	No sabe	2.38%
	Ninguno	7.14%
28-¿En su lugar de trabajo utiliza internet para acceder a la información que maneja?	Si	65.48%
	No	33.33%
	No sabe	1.19%
29-¿Cuál de las siguientes razones ha afectado el buen funcionamiento de su equipo informático? (selección múltiple)	Falta de limpieza rutinaria al equipo informático	65.48%
	Mala ubicación del equipo	10.71%
	Espacio reducido para la ubicación del equipo	23.81%
	Falta de aire acondicionado	35.71%
	Chispazos eléctricos en los tomacorrientes	17.86%
	Ninguna	14.29%
	Otros	3.57%
30-¿El equipo informático que almacena la información se encuentra expuesto a la afluencia de personas ajenas a la institución donde labora?	Si	11.90%
	No	88.10%

31-¿Su equipo informático ha presentado alguno de los siguientes fallos de rendimiento? (selección múltiple)	Lentitud	64.29%
	Congelamiento de pantallas	27.38%
	Apagones	25.00%
	Ninguno	23.81%
	Otros	1.19%
32-¿Qué tipo de mantenimiento se realiza en el equipo informático de su lugar de trabajo? (selección múltiple)	Preventivo	47.62%
	Correctivo	63.10%
	Ninguno	9.52%
	No sabe	3.57%

Fuente: Elaboración propia

3.1.3. Análisis de datos

Análisis de hipótesis 1

H1. Actualmente los usuarios que laboran en las instituciones no están capacitados adecuadamente en aspectos de seguridad sobre la información que manejan.

Ho1. Actualmente los usuarios que laboran en las instituciones están capacitados adecuadamente en aspectos de seguridad sobre la información que manejan.

Variable independiente: Usuarios no capacitados

Indicadores:

- **Recursos económicos**

Objetivo: Conocer si las instituciones públicas, empresas privadas y ONG´s, emplean recursos económicos para proteger sus bases de datos y redes informáticas.

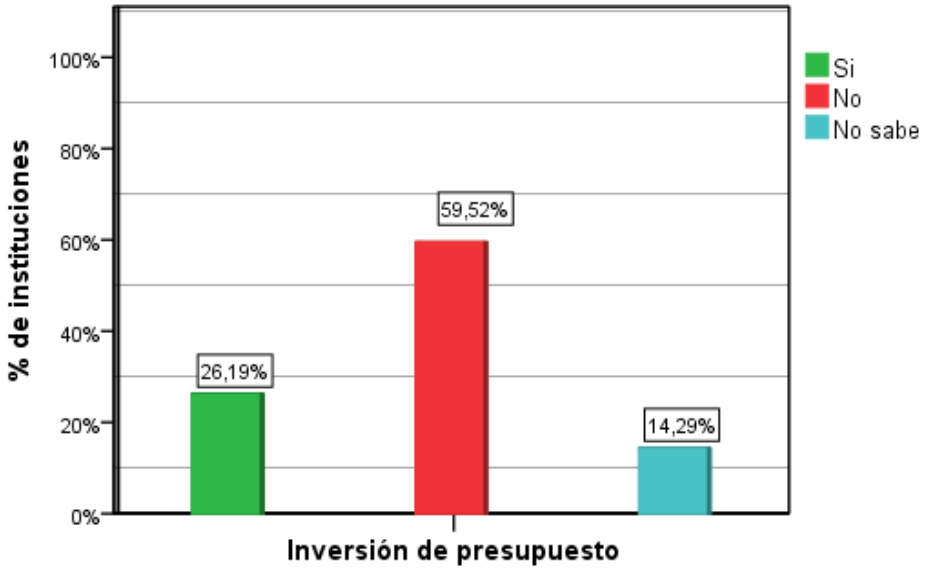
10-¿En el último año se ha invertido presupuesto en aspectos que contribuyan en la mejora de la seguridad de la información perteneciente a la institución donde labora?

Tabla 20: Inversión en aspectos para mejorar la seguridad de la información

Opciones	Frecuencia	Porcentaje
Si	22	26.2%
No	50	59.5%
No Sabe	12	14.3%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 11: Inversión en aspectos que ayuden a la mejora de la seguridad de información



Fuente: Elaboración propia

Análisis:

El estudio realizado nos indicó que la mayor parte de las instituciones encuestadas no incluían en su presupuesto aspectos de seguridad de las bases de datos y redes informáticas, el cual se representaba en un **59.52%**, esto indico que existía un problema debido a que no contaban con recursos económicos destinados a la seguridad informática por lo que se volvía una debilidad para las instituciones, ya que como se puede ver en la actualidad la tecnología crece cada día más y las amenazas se encuentran latentes, por lo que es necesario la protección de los datos y que el personal que maneja la información tenga conocimientos del buen uso que debe darle al equipo informático en que trabaja, las herramientas que utiliza y las medidas de seguridad que debe implementar para proteger la información que maneja, pero debido a que las instituciones no asignaban presupuesto para capacitar en el área de informática a dicho personal, estas se encontraban más expuestas a sufrir daños en sus activos. En cuanto a las instituciones que tenían asignado recursos económicos para mantener segura su información se representaba en un **26.19%** y el **14.29%** no sabía si contaban con recursos para invertir en dicha seguridad. Por lo que se concluyó que buena parte de las instituciones no contaban con una aplicación que les permitiera evaluar la seguridad de la información manejada, debido a que no estaban invirtiendo en este aspecto y los volúmenes de información varían de acuerdo a cada una de las instituciones.

- **Conocimientos de informática**

Objetivo: Conocer si las instituciones están capacitando periódicamente a su personal en aspectos de seguridad informática.

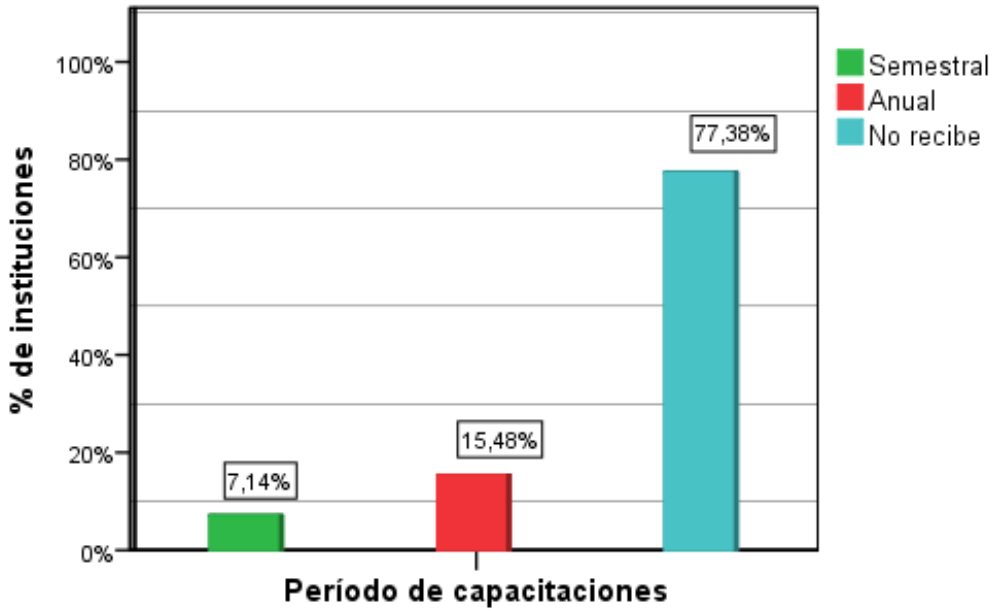
12-¿Cada cuánto tiempo recibe cursos de actualización sobre seguridad informática?

Tabla 21: Tiempo en el que reciben actualización sobre seguridad de la información

Opciones	Frecuencia	Porcentaje
Anual	13	15.5%
Semestral	6	7.1%
No recibe	65	77.4%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 12: Tiempo en el que reciben actualización de seguridad informática



Fuente: Elaboración propia

Análisis:

La gráfica muestra que el **77.38%** de las instituciones no capacitaban al personal sobre las actualizaciones de seguridad informática que se iban dando, lo cual nos indicó que estaban fallando en ese aspecto, ya que se estaban quedando desactualizados en cuanto a conocimientos que les pudieran ayudar a mejorar la seguridad de la información debido a que los usuarios de dichas instituciones no recibían cursos de seguridad informática y son ellos los que estaban directamente relacionados en el manejo de la información, por lo tanto debían estar debidamente capacitados para que pudieran explotar adecuadamente los recursos tecnológicos con que contaba la institución y así dar solución a problemas que se les presentaran ya sea en el manejo del equipo informático o en la herramienta que utilizaban para almacenar la información. En cuanto al resto de las instituciones, el **15.48%** capacitaba al personal anualmente y el **7.14%** lo hacían semestralmente, por lo que pudimos concluir que en la actualidad las instituciones encuestadas, en su mayoría contaban con personal no capacitado en aspectos de seguridad informática.

- **Disponibilidad de tiempo**

Objetivo: Identificar si los usuarios de las instituciones públicas, empresas privadas y ONG´s disponen de tiempo para recibir cursos de seguridad informática.

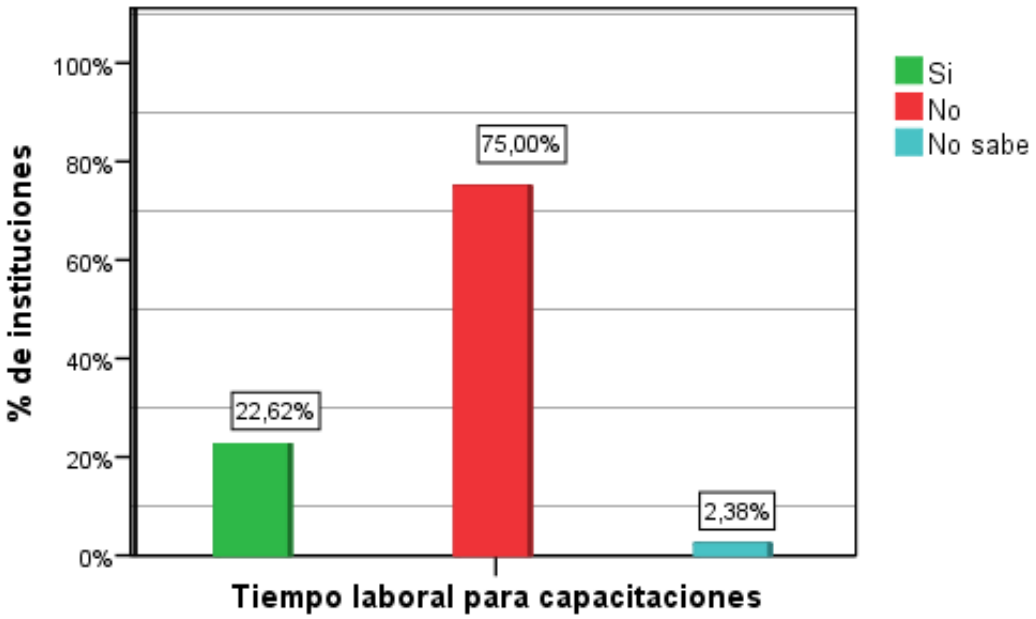
11-¿En su lugar de trabajo se asigna periódicamente parte del tiempo laboral, a capacitaciones sobre seguridad informática?

Tabla 22: Tiempo laboral de capacitaciones

Opciones	Frecuencia	Porcentaje
Si	19	22.6%
No	63	75.0%
No Sabe	2	2.4%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 13: Tiempo laboral destinado a capacitaciones sobre seguridad informática



Fuente: Elaboración propia

Análisis:

Se puede observar en la gráfica 13 que la mayoría de las instituciones no estaban asignando tiempo laboral para impartir capacitaciones sobre seguridad informática, este porcentaje estaba representado por un **75.00%**, por lo que se concluyó que los usuarios estaban trabajando a tiempo completo y por su carga laboral no tenían la disposición para actualizar sus conocimientos de informática.

Variable dependiente: Poca seguridad sobre la información que manejan

- **Políticas de seguridad implementadas**

Objetivo: Verificar si las instituciones implementan políticas de seguridad informática y si los usuarios que manejan la información tienen conocimientos de ellas.

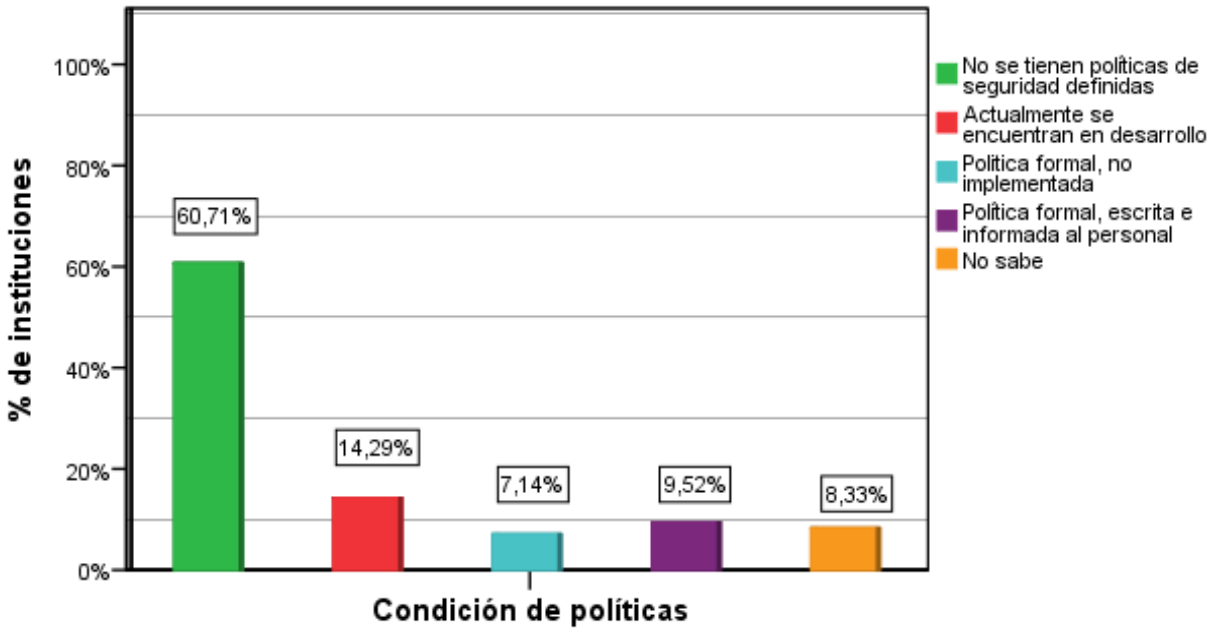
13-¿Cuál de las siguientes afirmaciones describe mejor la condición de las políticas de seguridad informática en su lugar de trabajo?

Tabla 23: Condición de políticas en la institución

Opciones	Frecuencia	Porcentaje
No se tienen políticas de seguridad definidas	51	60.7%
Actualmente se encuentran en desarrollo	12	14.3%
Política formal, no implementada	6	7.1%
Política formal, escrita e informada al personal	8	9.5%
No Sabe	7	8.3%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 14: Condición de políticas de seguridad informática en las instituciones



Fuente: Elaboración propia

Análisis:

Según los datos obtenidos se pudo observar en la gráfica 14 el **60.71%** que las instituciones no tenían políticas de seguridad informática definidas por lo que el personal las desconocía ya que el **8.33%** dijo que no sabían si existían dichas políticas y el **7.14%** dijo que existían pero que no se implementaban lo cual nos indicó que no se capacitaba o no se daba a conocer al usuario las reglas que debía aplicar para resguardar la información que manejaba y en cuanto a lo que debía y no debía hacer dentro de la institución. La falta de políticas conllevaba a que se cometieran actos que dañaran a la institución en general.

- **Uso inadecuado de herramientas o equipo**

Objetivo: Identificar si el personal que labora en las instituciones públicas, empresas privadas y ONG´s, hacen uso de herramientas para fines diferentes al de su trabajo.

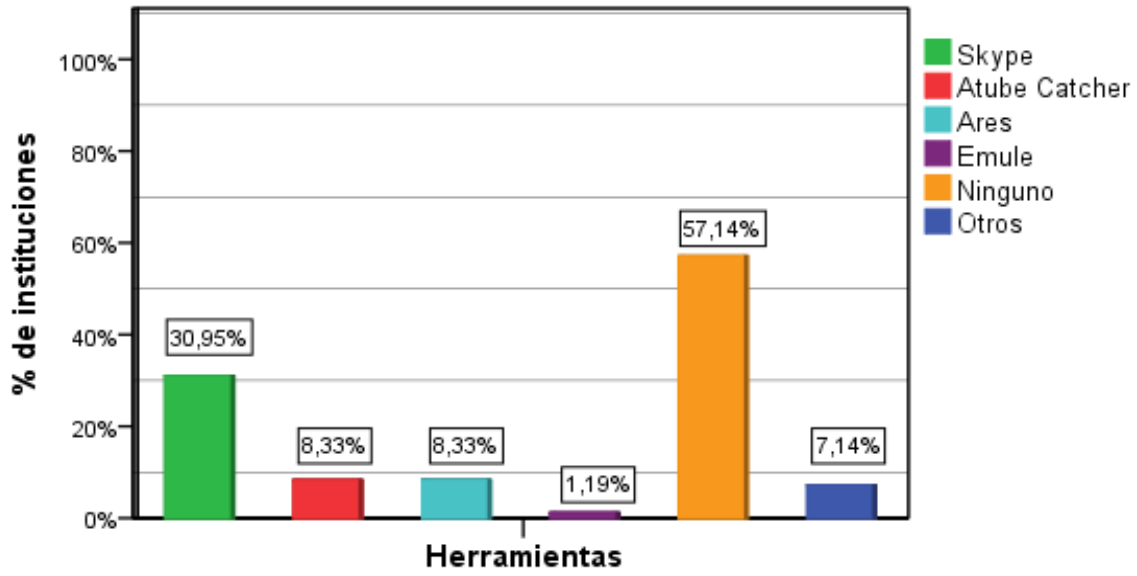
14-¿Hace uso de las siguientes herramientas en su equipo de trabajo?

Tabla 24: Herramientas de descargas utilizadas por usuarios de las instituciones

Opciones	Respuestas		Porcentaje de casos
	N°	Porcentaje	
Skype	26	27.4%	31.0%
Atube Catcher	7	7.4%	8.3%
Ares	7	7.4%	8.3%
Emule	1	1.1%	1.2%
Ninguno	48	50.5%	57.1%
Otros	6	6.3%	7.1%
Total	**95**	**100.0%**	**113.1%**

Fuente: Elaboración propia

Gráfica 15: Herramientas utilizadas por los usuarios en su trabajo



Fuente: Elaboración propia

Análisis:

Según los datos obtenidos se pudo observar que en las instituciones se estaban utilizando herramientas para uso personal lo cual indicaba que en dichas instituciones no se realizaba un monitoreo constante ignorando el uso de dichas herramientas y las desventajas que tenía el usarlas debido a que podía afectar la eficiencia de los usuarios que manejaban la información ya que se trataba de herramientas que distraían y con las cuales se podían contraer virus y dañar la información resguardada en el equipo de trabajo, tal como se muestra en la gráfica 15 el **30.95%** usaba Skype, el **8.33%** utilizaba Atube Cacher y Ares, y solo el **1.19%** Emule. A pesar que el **57.14%** de las instituciones encuestadas no utilizaban ninguna de dichas herramientas el resto si las estaban utilizando, por lo que las instituciones no estaban aplicando las medidas necesarias para evitar este tipo de uso y es por ello que era importante hacerles conciencia a los usuarios de que el hacer buen uso de las herramientas era parte de la seguridad que se le debía dar a la información que se manejaba. Por lo que se concluyó que estaban fallando en ese aspecto.

Análisis de hipótesis 2

H2. La pérdida de información de las instituciones se debe a la falta de aplicación de medidas de seguridad lógica.

Ho2. La pérdida de información de las instituciones no se debe a la falta de aplicación de medidas de seguridad lógica.

Variable independiente: Falta de aplicación de medidas de seguridad lógica

Indicadores:

- **Falta de conocimiento**

Objetivo: Identificar si la pérdida de la información perteneciente a las instituciones se debe a la falta de conocimientos sobre la aplicación de medidas de seguridad lógica por parte de los usuarios de la información.

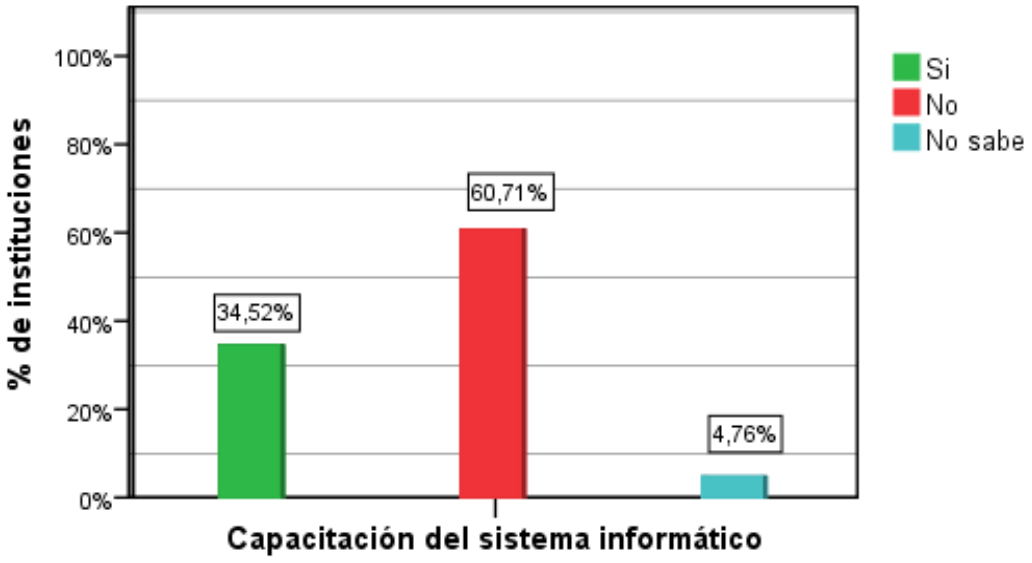
15-Cuándo se realizan actualizaciones en el sistema informático ¿Se imparten las capacitaciones necesarias?

Tabla 25: Capacitación cuando hay actualizaciones del sistema

Opciones	Frecuencia	Porcentaje
Si	29	34.5%
No	51	60.7%
No Sabe	4	4.8%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 16: Instituciones que capacitan cuando hay actualizaciones en el sistema



Fuente: Elaboración propia

Análisis:

El estudio realizado indicó que en las instituciones del departamento de San Vicente solo el **34.52%** estaban impartiendo las capacitaciones necesarias al personal luego de aplicar actualizaciones al sistema informático, y por la otra parte estaban las instituciones que no impartían capacitaciones luego de aplicar actualizaciones al sistema, representando a la gran mayoría con un **60.71%** lo que aumentaba las probabilidades de errores al ingresar los datos ya que sin una capacitación adecuada antes de utilizar el sistema actualizado, se estaba corriendo el riesgo que el personal cometiera errores con datos reales por no estar familiarizado con el sistema.

- **Falta de recurso económico**

Objetivo: Conocer si las instituciones están invirtiendo los recursos económicos necesarios en seguridad lógica para garantizar la seguridad de su información.

10-¿En el último año se ha invertido presupuesto en aspectos que contribuyan en la mejora de la seguridad de la información perteneciente a la institución donde labora?

Análisis:

La mayoría de las instituciones del departamento de San Vicente no estaban invirtiendo presupuesto en la mejora de la seguridad de la información y estaban representadas por un **59.52%,** del resto de instituciones el **14.29%** no sabían si se había invertido presupuesto en la mejora de la seguridad y solo un **26.19%** habían invertido presupuesto en la seguridad de la información en el último año. Esto mostro que más de la mitad de las instituciones del departamento de San Vicente no estaban asignando presupuesto a uno de los recursos más valiosos con los que contaba por lo que estaban dejando en segundo plano la seguridad de la información que manejaban lo que implicaba un gran costo y esfuerzo si esta sufriera daños o pérdidas irreparables por no aplicar las medidas de seguridad lógica por falta de presupuesto (ver gráfica 11, pág. 86).

- **Tipo de información manejada**

Objetivo: Verificar si las instituciones están clasificando su información en pública o privada como parámetro para proporcionar las medidas de seguridad lógica necesarias.

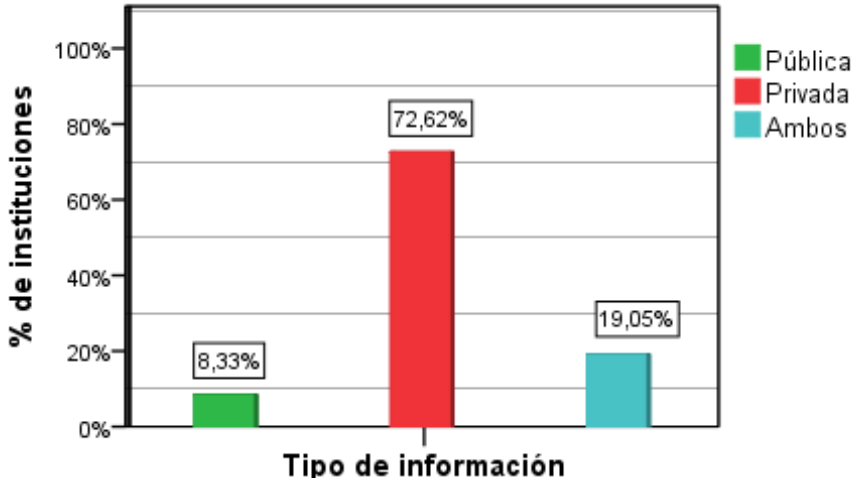
16-La información que maneja en su lugar de trabajo es de carácter:

Tabla 26: Tipo de información manejada por las instituciones

Opciones	Frecuencia	Porcentaje
Pública	7	8.3%
Privada	61	72.6%
Ambos	16	19.0%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 17: Tipo de información manejada por las instituciones



Fuente: Elaboración propia

Análisis:

Un **19.05%** de las instituciones manejan información tanto pública como privada, el **8.33%** de las instituciones manejan información únicamente de carácter público y el **72.62%** la clasifican como privada, esto nos indica que las instituciones necesitan medidas de seguridad para proteger la integridad de la información que está expuesta al público como también la información privada que necesita medidas lógicas de protección mucho más rigurosas.

- **Contraseña**

Objetivo: Identificar si las instituciones están utilizando contraseñas como mecanismo de seguridad lógica.

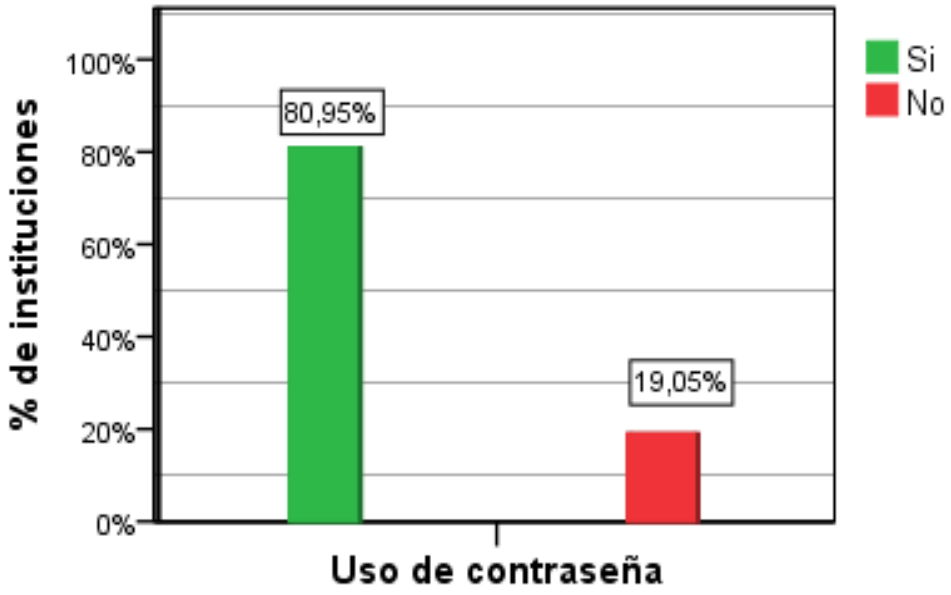
17-¿Utiliza contraseña para acceder a la información que almacena en su equipo de trabajo?

Tabla 27: Uso de contraseña

Opciones	Frecuencia	Porcentaje
Si	68	81.0%
No	16	19.0%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 18: Uso de contraseña en el acceso a la información



Fuente: Elaboración propia

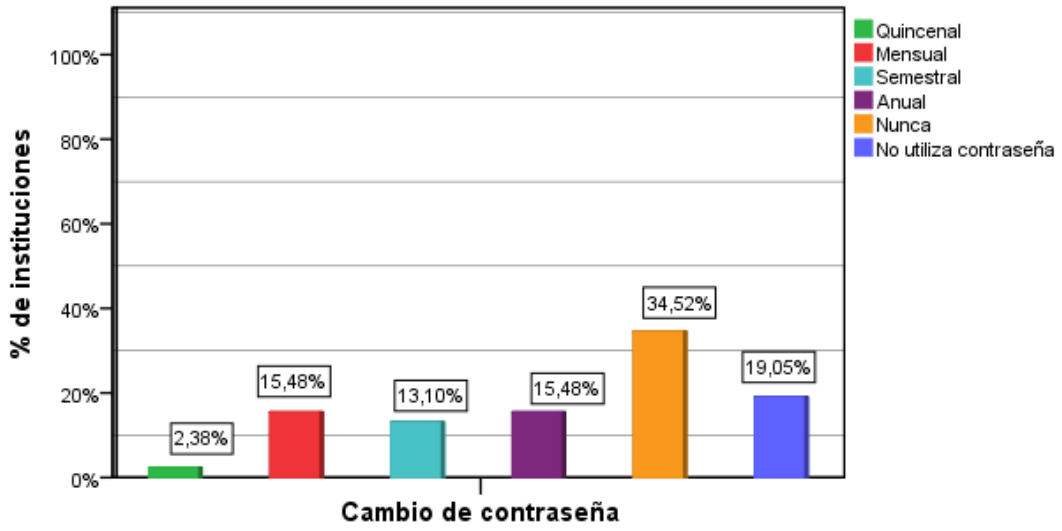
18-¿Cada cuánto tiempo cambia la contraseña de acceso a los datos que maneja en su lugar de trabajo?

Tabla 28: Cambio de contraseña

Opciones	Frecuencia	Porcentaje
Quincenal	2	2.4%
Mensual	13	15.5%
Semestral	11	13.1%
Anual	13	15.5%
Nunca	29	34.5%
No utiliza contraseña	16	19.0%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 19: Instituciones que cambian la contraseña de acceso a la información



Fuente: Elaboración propia

Análisis

Por medio de la investigación se identificó que **19.05%** de las instituciones no están utilizando contraseñas para acceder a la información y de las que si utilizan el **34.52%** nunca la cambian, el **15.48%** la cambian anualmente, el **13.10%** semestralmente, el **15.48%** mensualmente y solo el **2.38%** la cambia quincenalmente, esto nos indicó que en la mayoría de las instituciones se está pasando por alto cambiar la contraseña periódicamente y en las instituciones que la cambian lo hacen en periodos muy largos, esto se vuelve una desventaja ya que los intrusos que por algún motivo hayan obtenido la contraseña podrán hacer uso de esta durante largo tiempo, por lo que la falta de aplicación de esta medida de seguridad lógica afecta a las instituciones de San Vicente.

Variable dependiente: Poca seguridad sobre la información que manejan

- **Amenazas más comunes**

Objetivo: Identificar cuáles son las amenazas que más afectan la seguridad de la información que manejan las instituciones de san Vicente.

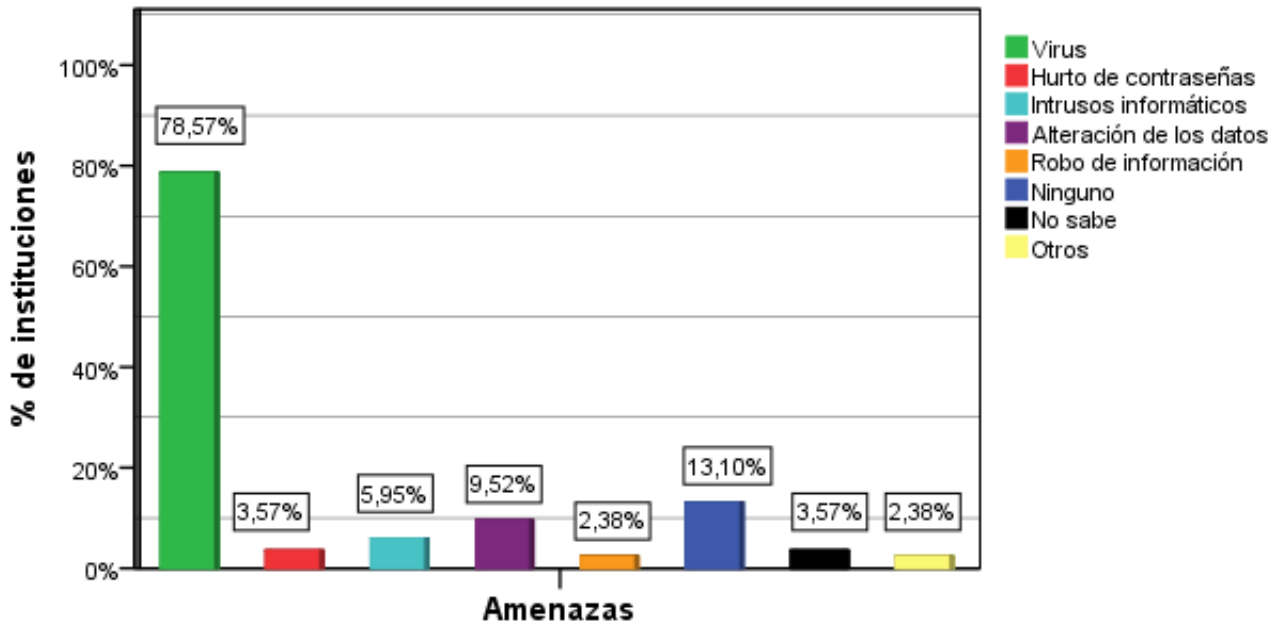
19-¿Se ha enfrentado a alguna de las siguientes amenazas de seguridad de la información? (selección múltiple)

Tabla 29: Amenazas identificadas en las instituciones

Opciones	Respuestas		Porcentaje de casos
	N°	Porcentaje	
Virus	66	66.0%	78.6%
Hurto de contraseñas	3	3.0%	3.6%
Intrusos informáticos	5	5.0%	6.0%
Alteración de los datos	8	8.0%	9.5%
Robo de información	2	2.0%	2.4%
No sabe	3	3.0%	3.6%
Ninguno	11	11.0%	13.1%
Otros	2	2.0%	2.4%
Total	**100**	**100.0%**	**119.0%**

Fuente: Elaboración propia

Gráfica 20: Amenazas que enfrentan las instituciones en la seguridad de la información



Fuente: Elaboración propia

Análisis:

La investigación demostró que la amenaza más frecuente para la información digital fueron los virus, la cual se presentó en un **78.57%** de las instituciones de San Vicente, además se pudieron identificar el hurto de contraseñas en un **3.57%,** los intrusos informáticos en un **5.95%,** la alteración de datos en un **9.52%** y el robo de información en un **2.38%,** siendo estas las amenazas más comunes que detectaron contra la seguridad de la información.

- **Copias de seguridad**

Objetivo: Identificar si las instituciones están creando respaldos de la información para evitar la pérdida de esta.

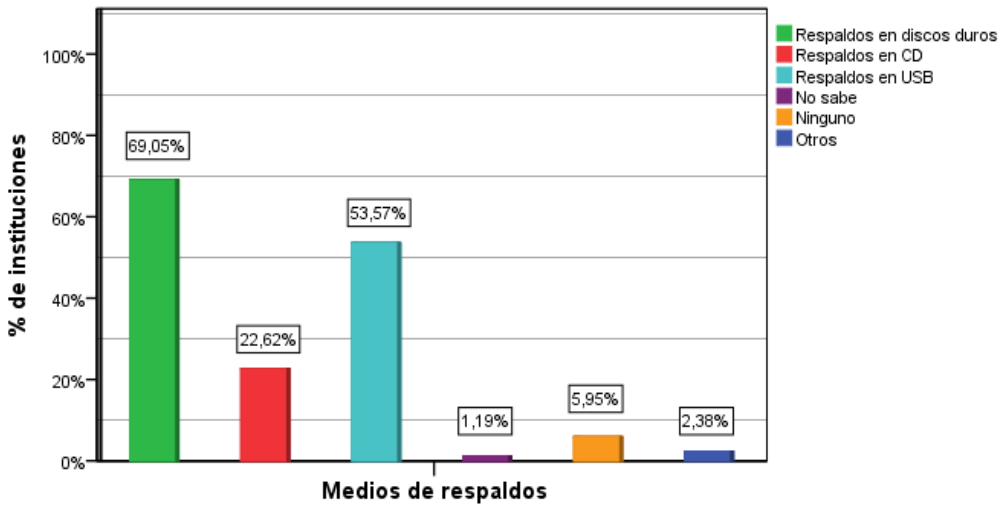
20-¿Cuáles de los siguientes medios utiliza actualmente en su lugar de trabajo para almacenar las copias de seguridad?

Tabla 30: Medios utilizados por las instituciones para respaldar la información

Opciones	Respuestas		Porcentaje de casos
	N°	Porcentaje	
Respaldos en discos duros	58	44.6%	69.0%
Respaldos en CD	19	14.6%	22.6%
Respaldos en USB	45	34.6%	53.6%
No sabe	1	.8%	1.2%
Ninguno	5	3.8%	6.0%
Otros	2	1.5%	2.4%
Total	**130**	**100.0%**	**154.8%**

Fuente: Elaboración propia

Gráfica 21: Medios que utilizan las instituciones para respaldar la información



Fuente: Elaboración propia

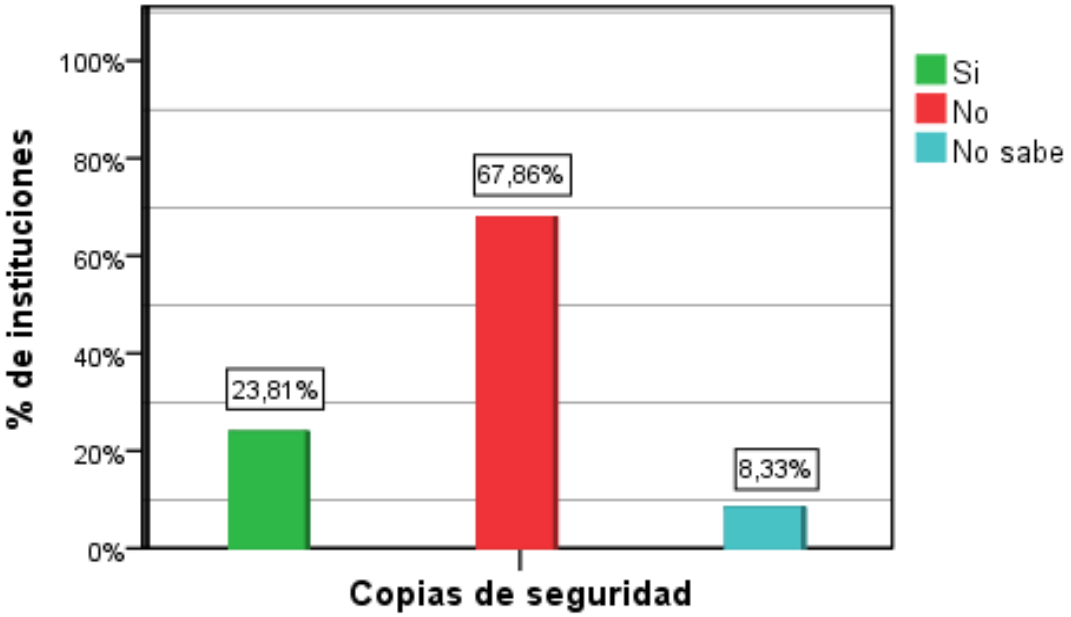
21-¿Se almacena alguna copia de seguridad fuera de los locales de trabajo?

Tabla 31: Copias fuera del local

Opciones	Frecuencia	Porcentaje
Si	20	23.8%
No	57	67.9%
No sabe	7	8.3%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 22: Instituciones que almacenan copias de seguridad fuera del local



Fuente: Elaboración propia

Análisis:

Aun cuando las instituciones estaban realizando copias de seguridad en diferentes medios no estaban considerando que algunos de los medios utilizados podían aumentar los riesgos de seguridad de la información como es el caso de las memorias USB, las cuales podían ser extraviadas o hurtadas fácilmente lo que aumentaba el riesgo de la información almacenada en ellas a pesar de esto el **53.57%** almacenaban sus copias de seguridad en dispositivos de este tipo, además se utilizaban CDs en un **22.62%** y el **69.05%** de las instituciones utilizaban discos duros para almacenar su información, pero más de la mitad de las instituciones que creaban copias de seguridad no guardaban un respaldo fuera de su lugar de trabajo, que garantizara la protección de la información en caso de desastres físicos que dañen total o parcialmente los contenedores de la información como podría ser un incendio, esta población estaba representada por el **67.86%** de las instituciones.

- **Antivirus**

Objetivo: Verificar si las instituciones están utilizando antivirus para evitar el contagio de virus que puedan poner en riesgo la información.

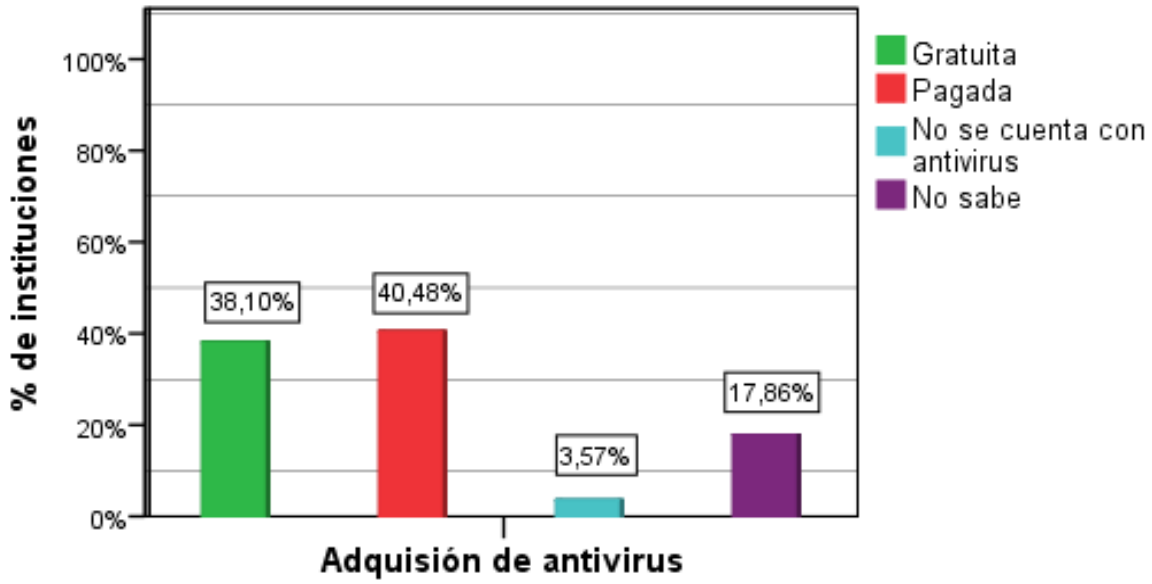
22-La versión del antivirus utilizado en la institución es:

Tabla 32: Tipo de adquisición de la versión del antivirus utilizado por las instituciones

Opciones	Frecuencia	Porcentaje
Gratuita	32	38.1%
Pagada	34	40.5%
No se cuenta con antivirus	3	3.6%
No sabe	15	17.9%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 23: Tipo de adquisición de la versión del antivirus utilizado por las instituciones



Fuente: Elaboración propia

Análisis:

El antivirus utilizado en las instituciones en un **38.10%** fue versión gratuita. Las versiones gratuitas tienen la desventaja de no tener todos los componentes de protección que normalmente trae una versión de antivirus pagado, vencen en periodos cortos de tiempo, comúnmente son descargados de páginas de internet que pueden infectar de virus a las computadoras. El **3.57%** no contaba con antivirus, el **17.86%** no sabían si la versión de su antivirus era gratuita o pagada y el **40.48%** tenía una versión de antivirus pagada. Por lo que casi la mitad de las instituciones no estaban dándole la importancia adecuada a contar con un antivirus que cumpla con el requisito mínimo de contar con una licencia, esto muestra una de las deficiencias de seguridad lógica que afectan a las instituciones de San Vicente.

Análisis de hipótesis 3

H3. Las instituciones no cuentan con un área informática interna que les brinde asistencia técnica inmediata.

Ho3. Las instituciones cuentan con un área informática interna que les brinde asistencia técnica inmediata.

Variable independiente: Falta de un área informática.

Indicadores:

- **Falta de recursos económicos**

Objetivo: Identificar si las instituciones públicas, privadas y ONG's de San Vicente poseen recursos económicos para la compra de equipo informático.

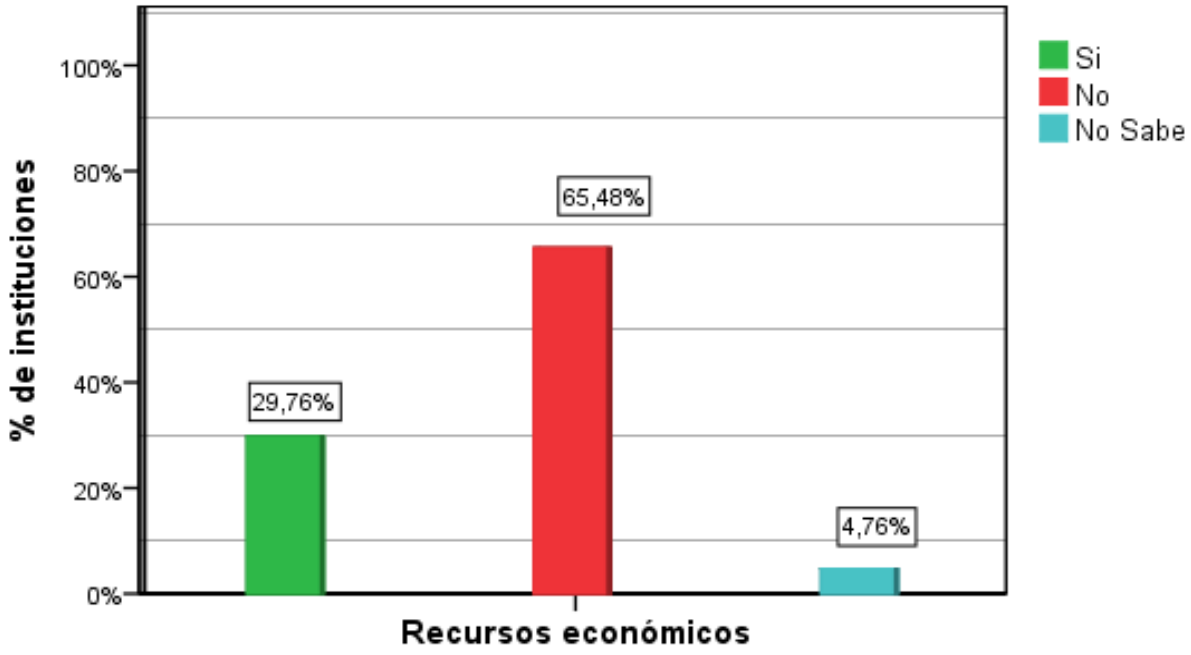
2 - ¿En su lugar de trabajo se cuenta con los recursos económicos para la compra de equipo informático?

Tabla 33: Recursos económicos

Opciones	Frecuencia	Porcentaje
Si	25	29.8%
No	55	65.5%
No Sabe	4	4.8%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 24: Instituciones que cuentan con recursos económicos para la compra de equipo informático



Fuente: Elaboración propia

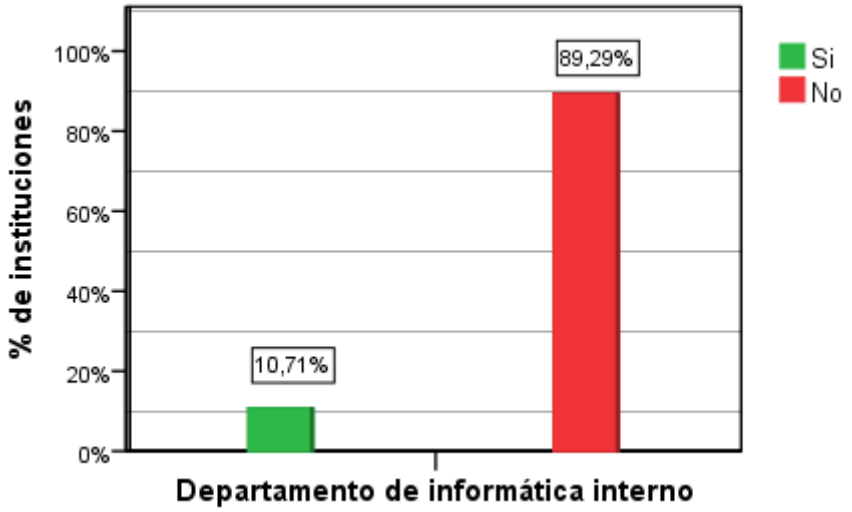
1-¿En su lugar de trabajo se cuenta con un departamento de informática interno?

Tabla 34: Departamento de informática interno

Opciones	Frecuencia	Porcentaje
Si	9	10.7%
No	75	89.3%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 25: Instituciones que cuentan con un departamento de informática interno



Fuente: Elaboración propia

Análisis:

Según los datos reflejados en la gráfica 25 una de las dificultades de las instituciones públicas, empresas privadas y ONG´s de San Vicente fue la ausencia de un departamento de informática interno, ya que solo el **10.71%** de las instituciones lo tenía, esto representaba un problema debido a que en muchas ocasiones las instituciones necesitaban de asistencia técnica inmediata.

Una razón por la que se determinó, la poca importancia que las instituciones le daban a la seguridad informática es la reducida asignación de recursos económicos que se le proporcionaban al departamento de informática pues se observa en la gráfica 24 que el **65.48%** de las instituciones no asignaban recursos para la compra de equipo informático. Si las instituciones no reciben asistencia técnica, mantenimiento preventivo y capacitación constante por ausencia de recursos económicos y de personal especializado en área informática determinamos que existe una necesidad de dar a conocer a las diferentes instituciones la importancia de invertir recursos económicos en el área de informática.

- **Asistencia técnica externa**

Objetivo: Determinar la procedencia de la asistencia técnica recibida por las instituciones públicas privadas y ONGs de san Vicente.

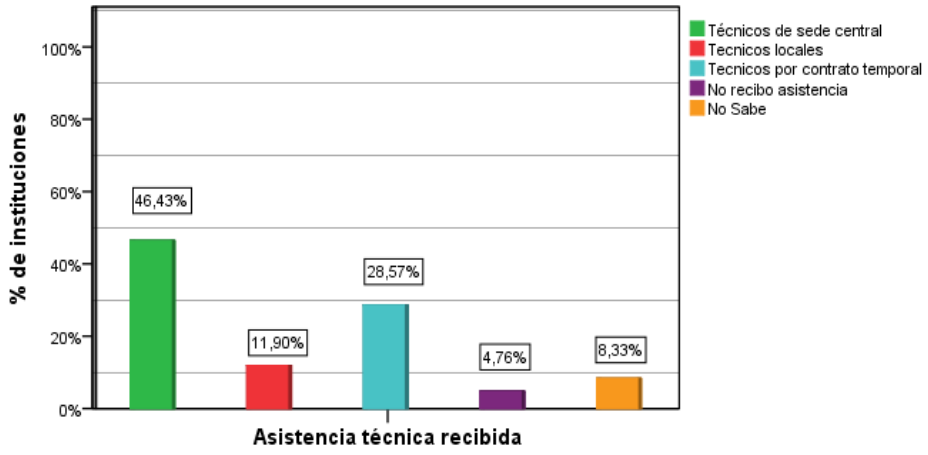
4-¿La asistencia técnica al equipo informático de su lugar de trabajo es proporcionada por?

Tabla 35: Asistencia técnica recibida

Opciones	Frecuencia	Porcentaje
Técnicos de sede central	39	46.4%
Técnicos locales	10	11.9%
Técnicos por contrato temporal	24	28.6%
No recibo asistencia	4	4.8%
No Sabe	7	8.3%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 26: Instituciones que reciben asistencia técnica



Fuente: Elaboración propia

Análisis:

En las instituciones había ausencia de personal especializado en el área de informática que tuviera conocimientos sobre aspectos de seguridad informática, como se muestra en la gráfica 26, solo un **11.90%** de las instituciones contaban con especialistas locales que les brindaban asistencia técnica inmediata, el resto de las instituciones recibían la asistencia técnica ya sea por técnicos de sede central o técnicos contratados temporalmente. Que las instituciones no contaran con un especialista local, que velara por los cuidados, capacitaciones y aspectos de seguridad de la información y del equipo informático de las instituciones, creaba deficiencias de seguridad en las instituciones y descuido en el equipo utilizado para almacenar las bases de datos.

Variable dependiente: No se brinda asistencia técnica inmediata.

- **Equipo adecuado:**

Objetivo: Verificar Si las Instituciones poseen las herramientas básicas para el mantenimiento de su equipo informático.

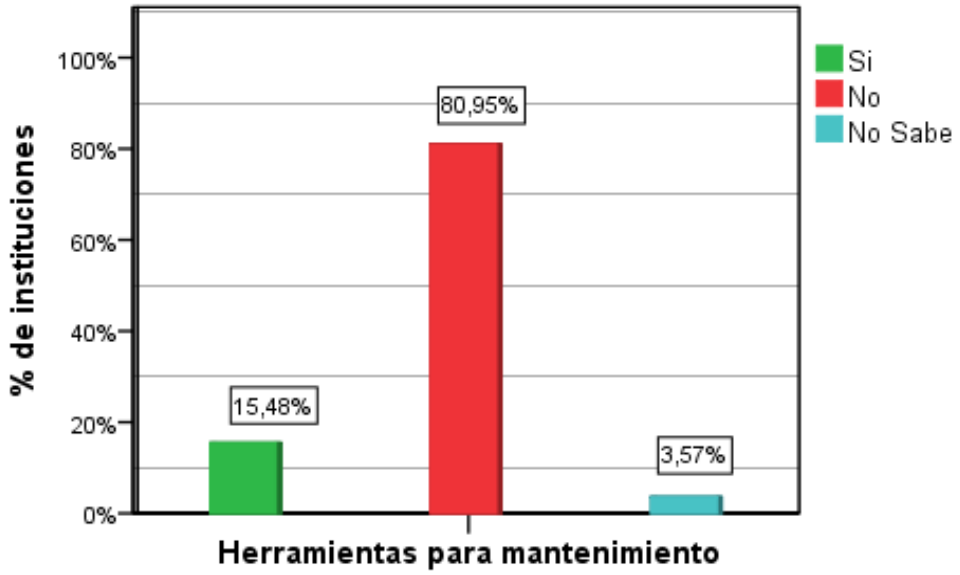
3-¿En su lugar de trabajo poseen herramientas para realizar el mantenimiento del equipo informático?

Tabla 36: Herramientas para mantenimiento

Opciones	Frecuencia	Porcentaje
Si	13	15.5%
No	68	81.0%
No Sabe	3	3.6%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 27: Instituciones que tienen herramientas para mantenimiento del equipo



Fuente: Elaboración propia

Análisis:

Para el buen funcionamiento del equipo informático es importante que este se encuentre en óptimas condiciones, por lo tanto es necesario que en las instituciones se cuente con las herramientas básicas para su mantenimiento ya sea preventivo o correctivo. En las instituciones de San Vicente solo el **15.48%** de las instituciones contaban con herramientas para dar mantenimiento a su equipo informático, el **80.95%** no contaban con dichas herramientas y el **3.57%** no sabía si las tenía.

- **Personal no capacitado**

Objetivo: Identificar si las instituciones públicas, privadas y ONG de San Vicente cuentan con personal especializado en informática.

4-¿La asistencia técnica al equipo informático de su lugar de trabajo es proporcionada por?

Análisis:

Según los datos obtenidos el **11.90%** de las instituciones recibía asistencia técnica por medio de técnicos locales, esta reflejaba el poco personal capacitado en el área de informática que contribuía periódicamente a capacitar e instruir al personal para que pudieran hacer el uso adecuado de las herramientas informáticas y para mantener la seguridad de la información, proporcionando mantenimiento al equipo informático de forma inmediata (ver gráfica 26, pág. 109).

- **Accesibilidad**

Objetivo: Identificar que tan accesible es para las instituciones recibir asistencia técnica en caso de fallos en la red o equipo informático.

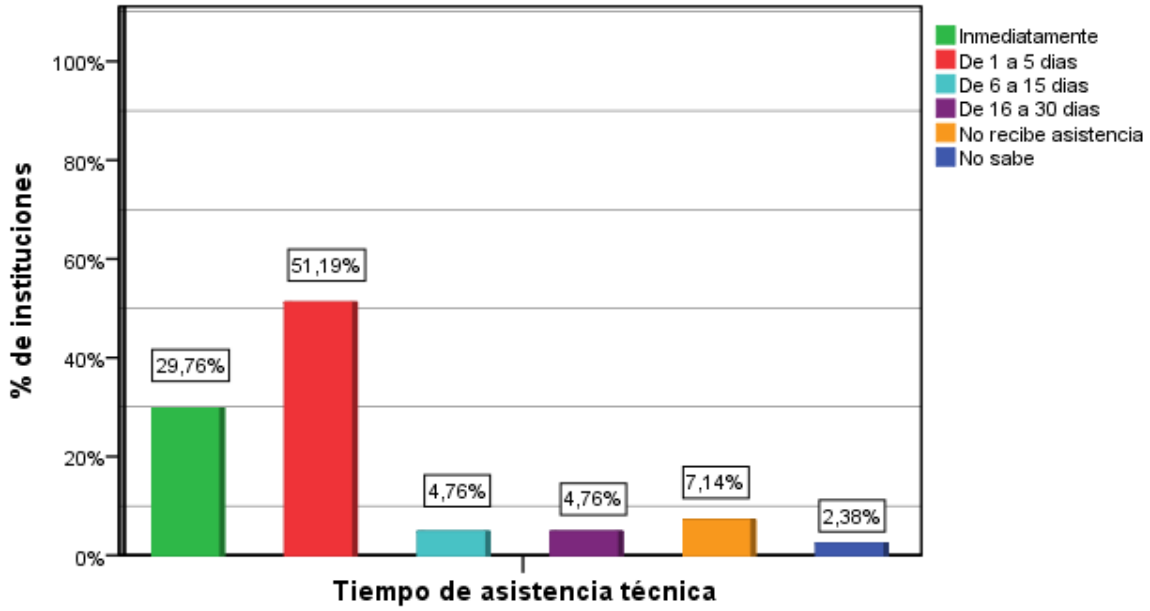
5-¿En caso de fallos en el equipo y/o en la red en cuanto tiempo aproximadamente recibe asistencia técnica?

Tabla 37: Tiempo de asistencia técnica

Opciones	Frecuencia	Porcentaje
Inmediatamente	25	29.8%
De 1 a 5 días	43	51.2%
De 6 a 15 días	4	4.8%
De 16 a 30 días	4	4.8%
No recibe asistencia	6	7.1%
No sabe	2	2.4%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 28: Tiempo que esperan las instituciones para recibir asistencia técnica



Fuente: Elaboración propia

Análisis:

En muchos aspectos el desarrollo de las actividades de las instituciones depende del buen funcionamiento del equipo, es por ello que cualquier daño que sufra el equipo en el que se almacena la información debe de ser atendido con rapidez, ya que al no ser atendido puede generar retrasos al usuario del equipo dañado. Según la gráfica 28 solo el **29.76%** de las instituciones contaban con asistencia técnica inmediata. El **51.19%** de las instituciones tenía que esperar entre 1 a 5 días para recibir asistencia técnica, el **4.76%** de 6 a 15 días y de 16 a 30 días y solo el **7.14%** no recibía. Esto representa una problemática debido a que en muchos casos las instituciones no tenían más equipo informático del que puedan disponer y esperar hasta que un especialista externo pueda brindar asistencia conllevaba al retraso del desarrollo de las actividades.

Análisis de hipótesis 4

H4. El equipo informático de las instituciones públicas, privadas y no gubernamentales se encuentra expuesto a riesgos físicos.

H4. El equipo informático de las instituciones públicas, privadas y no gubernamentales no se encuentra expuesto a riesgos físicos.

Variable independiente: Riesgos físicos

Indicadores:

- **Infraestructura**

Objetivo: Identificar los problemas de infraestructura que podrían ser un riesgo para el equipo informático de las instituciones de San Vicente.

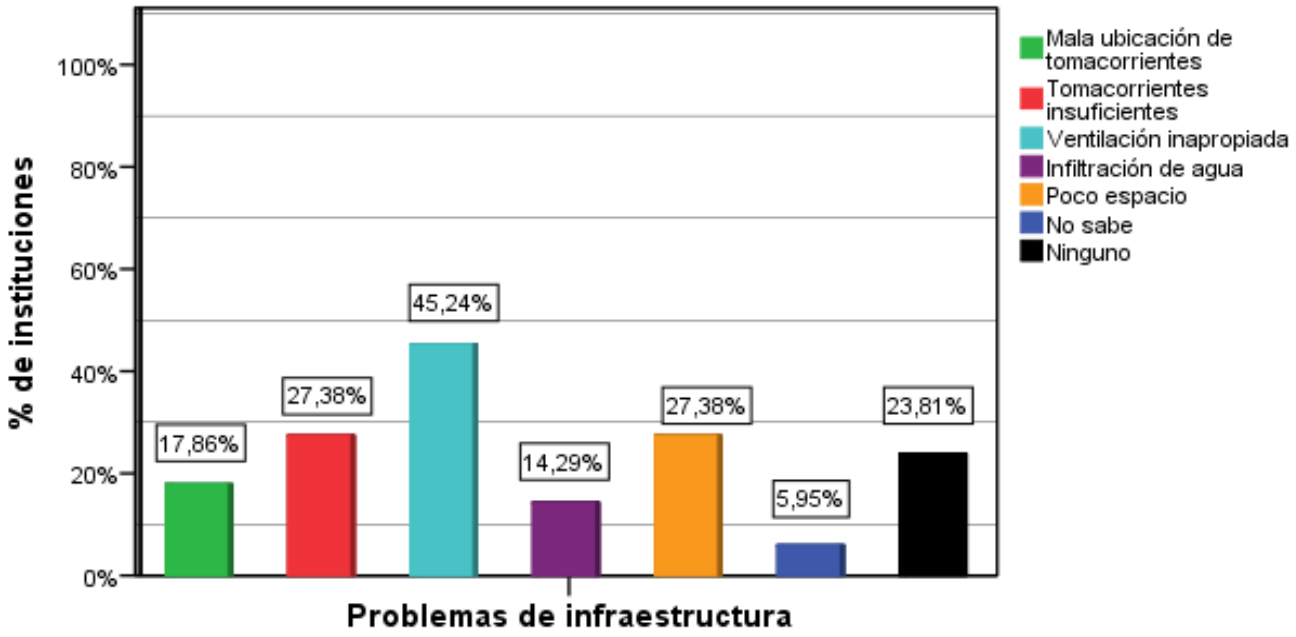
23-¿Seleccione los problemas de infraestructura que representan riesgo para los equipos que almacenan la información en su lugar de trabajo? (selección múltiple)

Tabla 38: Problemas de infraestructura

Opciones	Respuestas		Porcentaje de casos
	N°	Porcentaje	
Mala ubicación de tomacorrientes	15	11.0%	17.9%
Tomacorrientes insuficientes	23	16.9%	27.4%
Ventilación inapropiada	38	27.9%	45.2%
Infiltración de agua	12	8.8%	14.3%
Poco espacio	23	16.9%	27.4%
No sabe	5	3.7%	6.0%
Ninguno	20	14.7%	23.8%
Total	**136**	**100.0%**	**161.9%**

Fuente: Elaboración propia

Gráfica 29: Problemas de infraestructura en las instituciones



Fuente: Elaboración propia

Análisis:

Se identificó que las instituciones tenían problemas de infraestructuras entre ellas el **45.24%** tenía ventilación inapropiada, el **27.38%** no contaba con suficientes tomacorrientes y tenían poco espacio, el **17.86%** dijo que un problema era la mala ubicación de tomacorrientes y el **14.29%** la infiltración de agua. Todos estos factores representaban un riesgo físico para el equipo de trabajo ya que si no se tiene una adecuada ventilación puede provocar un sobrecalentamiento al equipo, que no se tengan suficientes tomacorrientes y la mala ubicación de estos dificulta la conexión del equipo informático necesario para el registro y almacenamiento de la información, el poco espacio conlleva a que se den accidentes y de igual forma la infiltración de agua puede ocasionar daños al equipo en caso de que este se encuentre cerca del problema.

- **Sobrecalentamiento del equipo**

Objetivo: Identificar si el equipo informático perteneciente a las instituciones de San Vicente se han visto afectados por problemas de sobrecalentamiento.

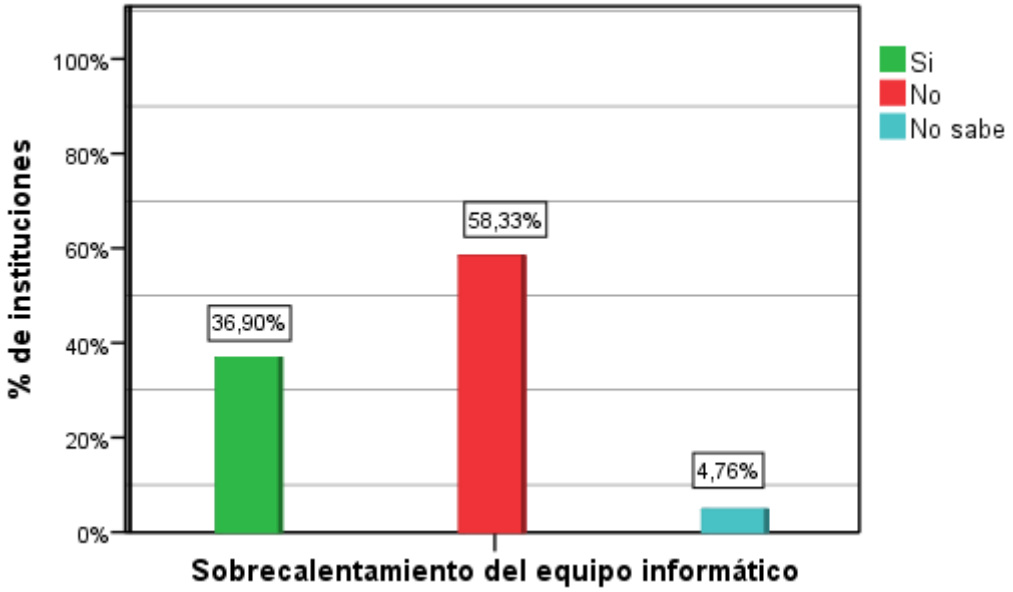
24-¿El equipo Informático en que trabaja ha presentado problemas de sobrecalentamiento?

Tabla 39: Problemas de sobrecalentamiento

Opciones	Frecuencia	Porcentaje
Si	31	36.9%
No	49	58.3%
No sabe	4	4.8%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 30: Problemas de sobrecalentamiento del equipo informático de las instituciones



Fuente: Elaboración propia

Análisis:

La gráfica 30 refleja que el **36.90%** de las instituciones han tenido problemas de sobrecalentamiento del equipo informático, lo que nos indicó que el equipo no estaba en condiciones adecuadas, por lo que es importante que el lugar donde se encuentre el equipo informático este acondicionado adecuadamente para evitar que se recaliente debido a las altas temperaturas y así mantener fuera de este riesgo la información que se resguarda en él, dado que el sobrecalentamiento puede provocar que algunos dispositivos de la computadora puedan quemarse dejando el equipo fuera de uso repentinamente.

- **Delincuencia**

Objetivo: Conocer si las instituciones se han enfrentado a problemas de robo de equipo informático por culpa de la delincuencia.

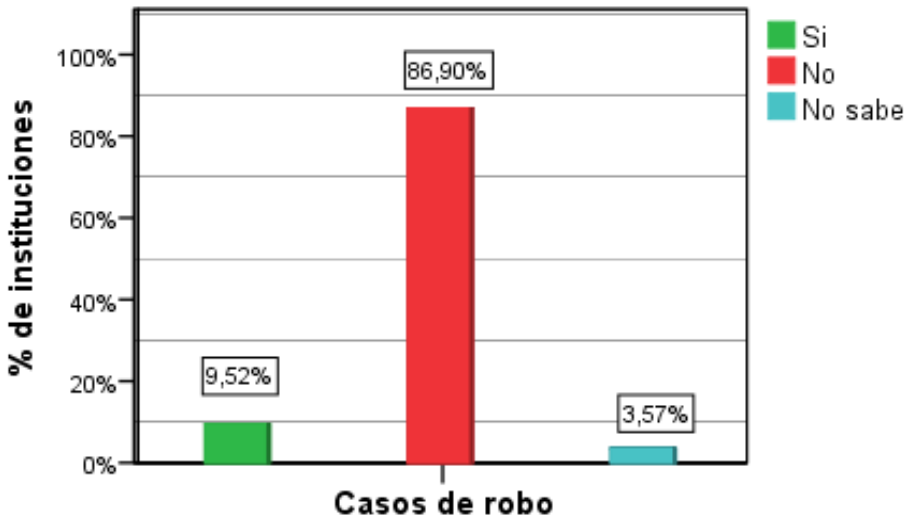
25-¿En su lugar de trabajo se han presentado casos de robo de equipo informático?

Tabla 40: Robo de equipo informático

Opciones	Frecuencia	Porcentaje
Si	8	9.5%
No	73	86.9%
No sabe	3	3.6%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 31: Robo de equipo informático en las instituciones



Fuente: Elaboración propia

Análisis:

Según los datos reflejados en la gráfica 31 solo en un **9.52%** de las instituciones se presentaron casos de robo de equipo informático, y a pesar que el porcentaje es mínimo indico que todas las empresas corren el riesgo de perder equipo informático debido a los altos índices de delincuencia que se presentan en la actualidad, en cuanto el **86.90%** no se ha enfrentado a casos de robo, pero el hecho que no se hayan enfrentado a este tipo de problema no significa que no estén expuestas pues se trata de un factor que esta fuera de nuestro control por lo que se debe estar prevenidos y mantener seguridad en las instalaciones.

Variable dependiente: Vulnerabilidad del equipo informático.

Indicadores:

- **Vida útil**

Objetivo: Identificar si las instituciones están utilizando computadoras que han excedido su vida útil.

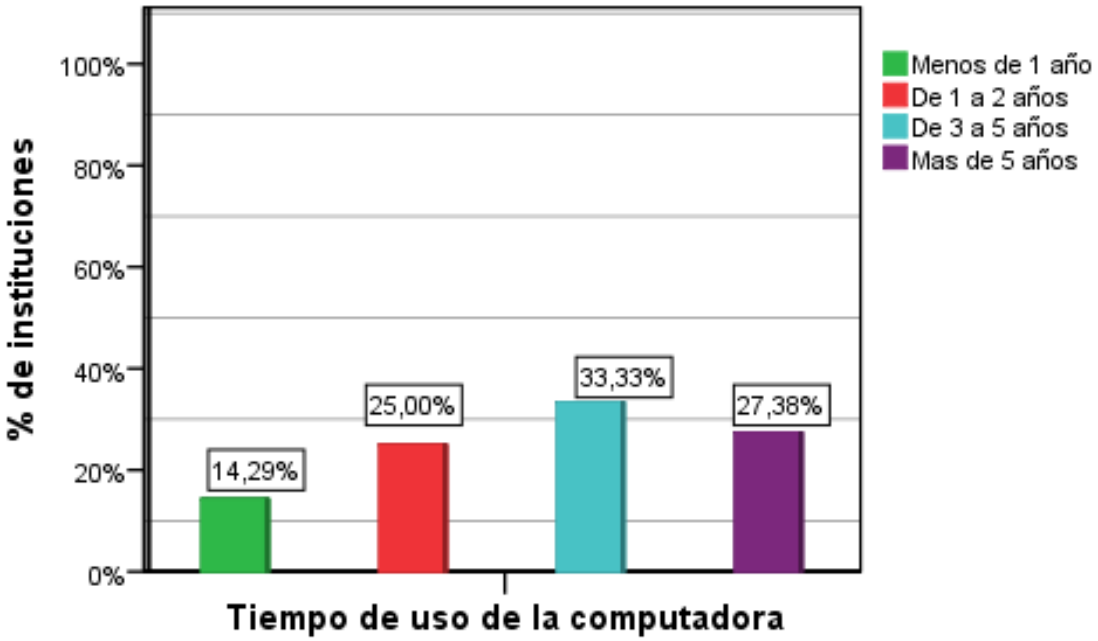
26-¿Aproximadamente cuánto tiempo tiene de uso la computadora en que trabaja?

Tabla 41: Tiempo de uso de la computadora

Opciones	Frecuencia	Porcentaje
Menos de 1 año	12	14.3%
De 1 a 2 años	21	25.0%
De 3 a 5 años	28	33.3%
Más de 5 años	23	27.4%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 32: Tiempo de uso del equipo informático utilizado en las instituciones



Fuente: Elaboración propia

Análisis:

La grafica demuestra que más de la mitad de las instituciones estaban utilizando computadoras con vida útil excedida, considerando como vida útil un límite de dos años, el porcentaje está representado por un **33.33%** y **27.38%** de instituciones que tenían computadoras con tiempo de uso entre 3 y 5 años y con más de 5 años, lo que puede producir fallos en estas por el desgaste generado por el tiempo de uso.

- **Acondicionamiento**

Objetivo: Identificar si las instituciones de San Vicente están trabajando en condiciones que presenten algún problema de acondicionamiento que ponga en riesgo el equipo informático.

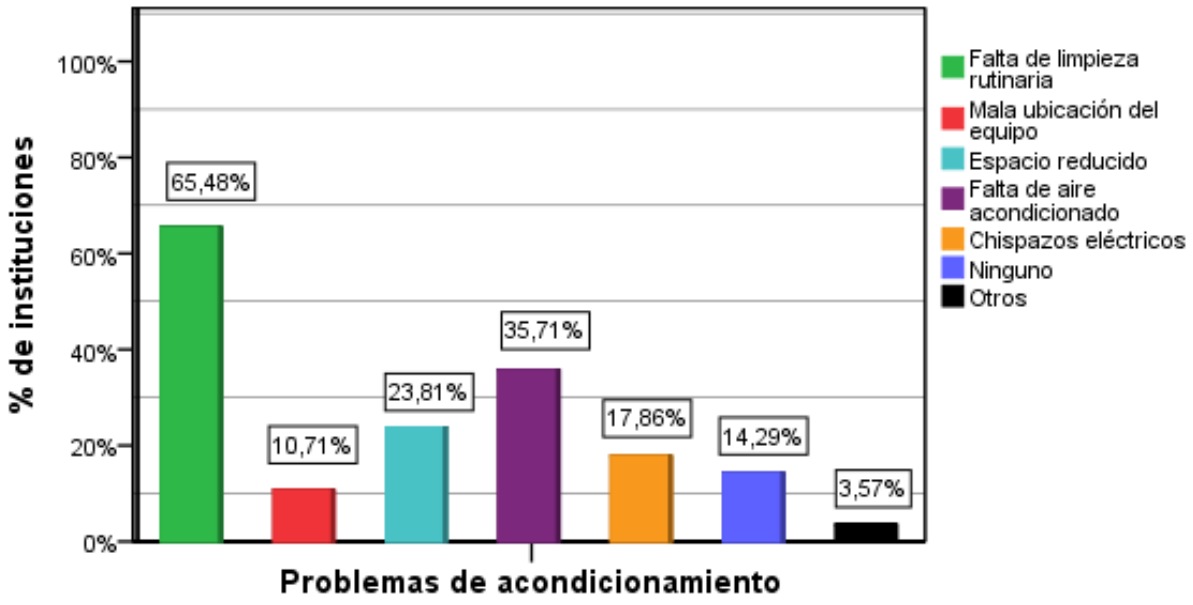
29-¿Cuál de las siguientes razones ha afectado el buen funcionamiento de su equipo informático? (selección múltiple)

Tabla 42: Razones que afectan el buen funcionamiento del equipo informático

Opciones	Respuestas		Porcentaje de casos
	N°	Porcentaje	
Falta de limpieza rutinaria	55	38.2%	65.5%
Mala ubicación del equipo	9	6.3%	10.7%
Espacio reducido	20	13.9%	23.8%
Falta de aire acondicionado	30	20.8%	35.7%
Chispazos eléctricos	15	10.4%	17.9%
Ninguna	12	8.3%	14.3%
Otras	3	2.1%	3.6%
Total	**144**	**100.0%**	**171.4%**

Fuente: Elaboración propia

Gráfica 33: Razones que afectan a los equipos informáticos de las instituciones



Fuente: Elaboración propia

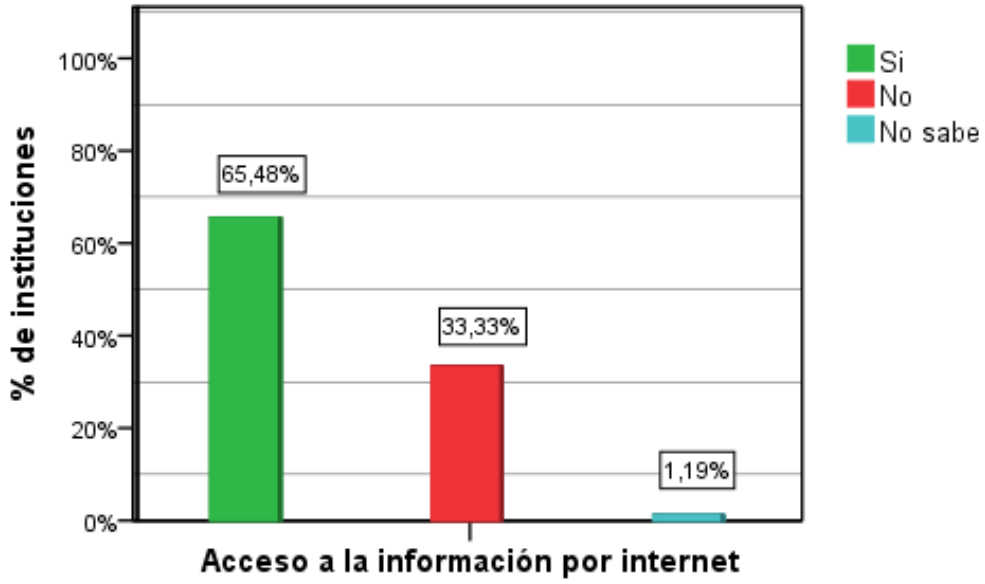
28-¿En su lugar de trabajo utiliza internet para acceder a la información que maneja?

Tabla 43: Acceso a la información por internet

Opciones	Frecuencia	Porcentaje
Si	55	65.5%
No	28	33.3%
No sabe	1	1.2%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 34: Instituciones que utilizan internet para el acceso a la información



Fuente: Elaboración propia

Análisis:

En la gráfica 33 podemos observar algunos de los problemas de acondicionamiento que estaban afectando el equipo informático de las instituciones de San Vicente, en primer lugar está la falta de limpieza al equipo informático, afectando a un **65.48%** de las instituciones, esto podría producir acumulación de polvo en los equipos, afectando el buen funcionamiento del equipo, en segundo lugar con un **10.71%** se tenía la mala ubicación del equipo, que puede afectar la eficacia del personal pudiendo estar más propenso a cometer errores ya sea por un reflejo en la pantalla, que una impresora este demasiado retirada del sitio donde se da la orden de impresión entre otros, luego se tenía el espacio reducido con un **23.81%**, este problema aumenta la probabilidad que se produzcan accidentes debido al espacio reducido, pudiendo golpear con objetos al equipo mientras las personas se desplazan de un lugar a otro, además otro problema detectado es la falta de aire acondicionado, que afectaba a un **35.71%** de las instituciones, esto sumado a las largas horas de trabajo a las que se exponía el equipo podría provocar sobrecalentamientos, y por último con un **17.86%** se tienen los chispazos eléctricos producidos en los tomacorrientes, que podrían deberse a deterioros en las instalaciones eléctricas, por defectos en la instalación entre otras razones,

estos chispazos provocan variabilidad en la energía eléctrica que podría dañar a los equipo al conectarlos.

Además se puede observar en la gráfica 34 que un **65.48%** de las instituciones utilizaban internet para trasmitir información laboral esto sería una ventaja si se tuvieran las medidas de seguridad apropiadas, pero si no se restringen los sitios web de ocio el internet puede ser un gran distractor y transmisor de virus.

- **Ubicación**

Objetivos: Conocer si el equipo informático donde se resguarda la información perteneciente a las instituciones de San Vicente se encuentra expuesto a personas ajenas a la institución.

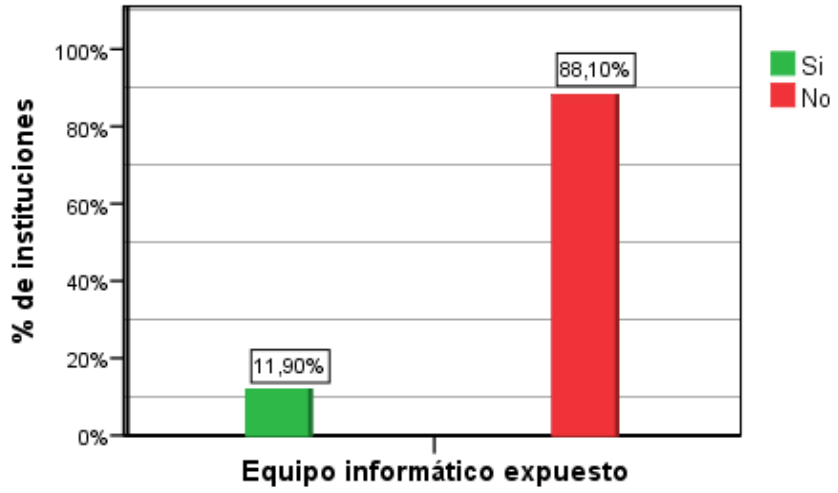
30-¿El equipo informático que almacena la información se encuentra expuesto a la afluencia de personas ajenas a la institución donde labora?

Tabla 44: Equipo expuesto a la afluencia de personas

Opciones	Frecuencia	Porcentaje
Si	10	11.9
No	74	88.1
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 35: Equipo informático expuesto a la afluencia de personas ajenas



Fuente: Elaboración propia

Análisis:

Las instituciones que tenían su equipo informático expuesto a la afluencia de personas era el **11.90%**, este porcentaje es relativamente pequeño pero al tener el equipo demasiado expuesto a personas ajenas a la institución vuelve más vulnerable la información almacenada ya sea a modificaciones no autorizadas o hurtos.

- **Capacidad**

Objetivos: Identificar si las instituciones de San Vicente tienen el equipo informático con la capacidad necesaria para garantizar que no se ocasionen inconvenientes mientras se manipula la información.

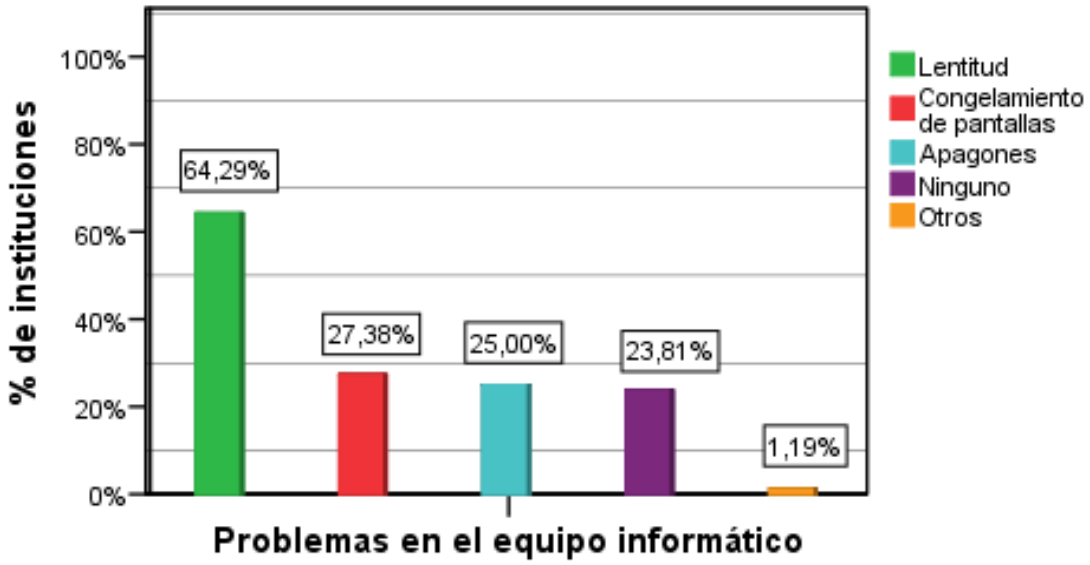
31-¿Su equipo informático ha presentado alguno de los siguientes fallos de rendimiento? (selección múltiple)

Tabla 45: Fallos de rendimiento en el equipo informático

Opciones	Respuestas		Porcentaje de casos
	N°	Porcentaje	
Lentitud	54	45.4%	64.3%
Congelamiento de pantallas	23	19.3%	27.4%
Apagones	21	17.6%	25.0%
Ninguno	20	16.8%	23.8%
Otros	1	0.8%	1.2%
Total	**119**	**100.0%**	**141.7%**

Fuente: Elaboración propia

Gráfica 36: Problemas que han tenido las instituciones en el equipo informático



Fuente: Elaboración propia

Análisis:

En el estudio realizado se pudo detectar una cantidad de problemas que se relacionan con la capacidad del hardware utilizado en las instituciones, el primer problema detectado fue la lentitud en las computadoras con un **64.29%**, como segundo problema se identificó el congelamiento de pantallas con un **27.38%**, que se producían por el deterioro del equipo, el tercer problema identificado fue los apagones en el equipo con un **25.00%** este problema es frecuente que se produzca en la última etapa funcional del equipo, todos estos fallos afectan el funcionamiento óptimo del equipo poniendo en riesgo la información almacenada.

- **Mantenimiento al equipo**

Objetivos: Identificar cual es el tipo de mantenimiento que se le da al equipo informático de las instituciones de San Vicente.

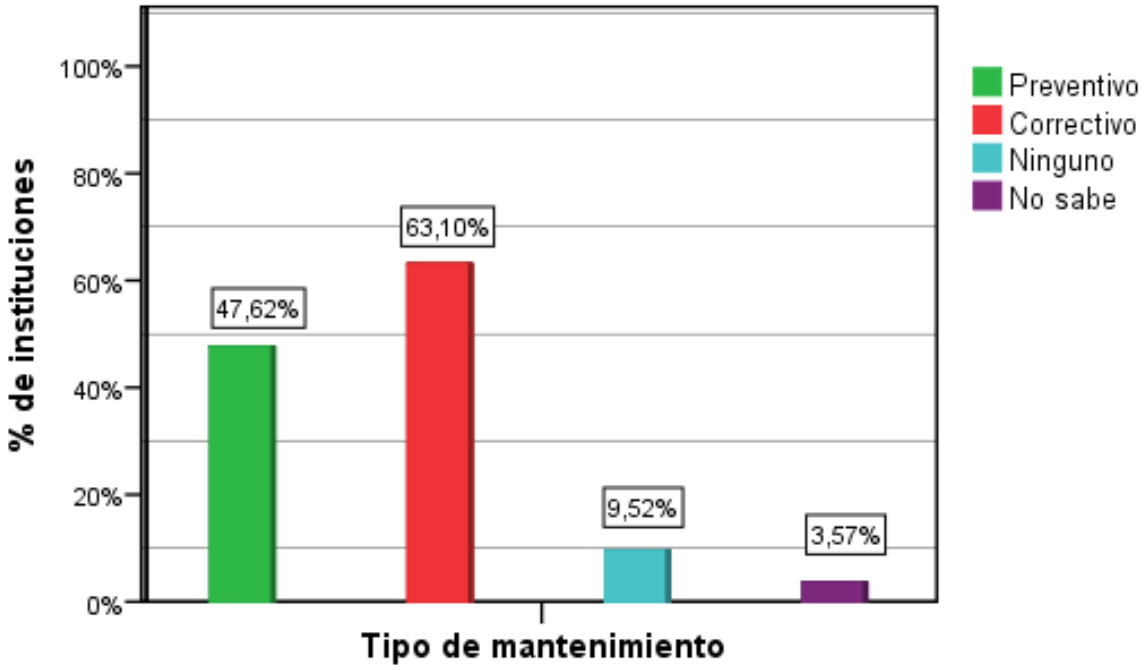
32-¿Qué tipo de mantenimiento se realiza en el equipo informático de su lugar de trabajo? (selección múltiple)

Tabla 46: Tipo de mantenimiento que se le da al equipo informático

Opciones	Respuestas		Porcentaje de casos
	N°	Porcentaje	
Preventivo	40	38.5%	47.6%
Correctivo	53	51.0%	63.1%
Ninguno	8	7.7%	9.5%
No sabe	3	2.9%	3.6%
Total	**104**	**100.0%**	**123.8%**

Fuente: Elaboración propia

Gráfica 37: Tipo de mantenimiento que se le da al equipo informático de las instituciones



Fuente: Elaboración propia

Análisis:

Las instituciones de San Vicente en su mayoría efectuaban mantenimiento correctivo al equipo, representando un **63.10%**, el **47.62%** de las instituciones realizaban mantenimiento preventivo, el **9.52%** no realizaban ningún tipo de mantenimiento y el **3.57%** no sabían si se realiza mantenimiento. Que las instituciones no estuvieran realizando mantenimiento o que lo hicieran únicamente de manera correctiva aumentaba las probabilidades que el equipo fallara en un periodo más temprano al normal de un equipo al que se le brinda el mantenimiento adecuado, un fallo inesperado por falta de mantenimiento puede causar pérdidas de información en el sistema.

Análisis de hipótesis general

Hg. En la Actualidad, las Instituciones públicas, privadas y no gubernamentales del departamento de San Vicente, tienen la necesidad de una herramienta informática de evaluación que les permitan determinar el nivel de seguridad en sus bases de datos y redes informáticas.

Ho. En la Actualidad, las Instituciones públicas, privadas y no gubernamentales del departamento de San Vicente, no tienen la necesidad de una herramienta informática de evaluación que les permitan determinar el nivel de seguridad en sus bases de datos y redes informáticas.

Variable independiente: Falta de herramienta informática de evaluación.

Indicadores:

- **Bajo presupuesto**

Objetivo: Verificar si las instituciones actualmente han invertido presupuesto en la compra de programas informáticos.

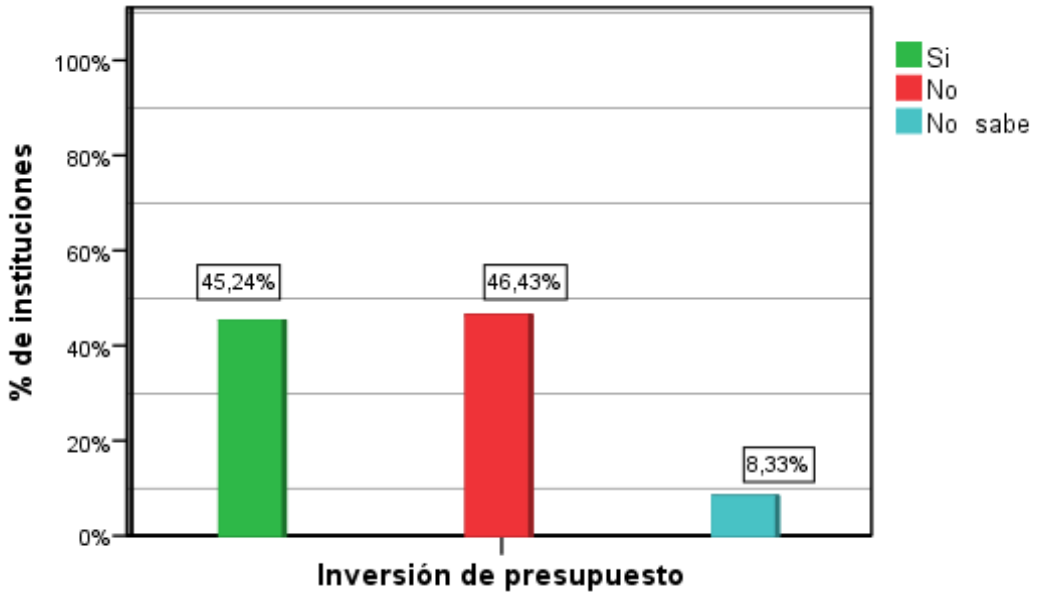
6-¿En su lugar de trabajo se ha invertido presupuesto en los últimos dos años en la compra de programas informáticos actualizados?

Tabla 47: Inversión de presupuesto en la compra de programas

Opciones	Frecuencia	Porcentaje
Si	38	45.2%
No	39	46.4%
No Sabe	7	8.3%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 38: Instituciones que han invertido en la compra de programas informáticos



Fuente: Elaboración propia

Análisis:

Según los datos obtenidos de todas las instituciones encuestadas el **46.43%** no había invertido presupuesto en los dos últimos años en la compra de programas informáticos, lo cual indicaba que carecían de herramientas informáticas actualizadas, entre ellas una que les permitiera medir el nivel de seguridad en sus bases de datos y redes informáticas debido a que el porcentaje de instituciones antes mencionadas no contaban con suficientes recursos económicos para obtener dichas herramientas, el **45.24%** de las instituciones las habían adquirido, y un **8.33%** no sabían si se ha invertido en la compra de dichas herramientas.

- **Criterios de evaluación**

Objetivo: Identificar si en las instituciones públicas, empresas privadas y ONG´s implementan criterios de evaluación para evaluar al personal sobre la seguridad de la información que maneja en la computadora.

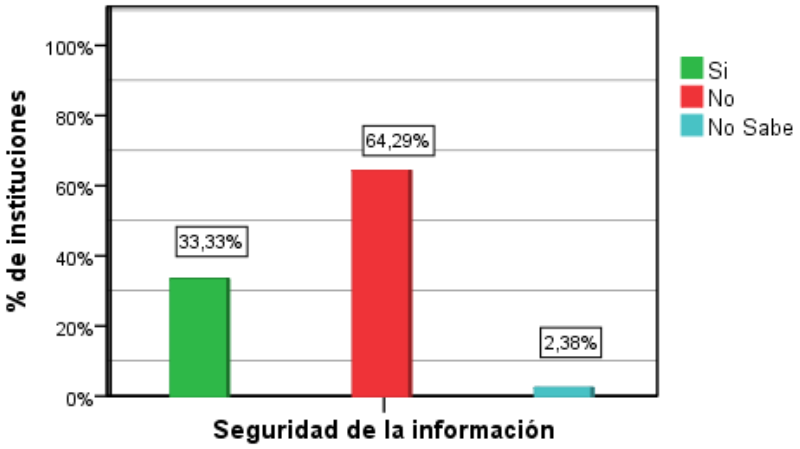
7-¿En su lugar de trabajo le evalúan la seguridad con que maneja la información almacenada digitalmente?

Tabla 48: Evaluación de la seguridad

Opciones	Frecuencia	Porcentaje
Si	28	33.3%
No	54	64.3%
No Sabe	2	2.4%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 39: Instituciones que evalúan la seguridad de la información



Fuente: Elaboración propia

Análisis:

En la gráfica 39 se puede observar que en su mayoría, representada por el **64.29%** de las instituciones no estaban evaluando a su personal en cuanto a la seguridad de la información digital, esto generaba muchas desventajas debido a que el personal es quien estaba directamente relacionado con el registro de información y al no implementar criterios para evaluarlo generaba un punto débil en la seguridad de la información, ya que no se tomaban las medidas necesarias para verificar si las funciones se estaban desempeñando

adecuadamente, por lo que es de mucha utilidad que las instituciones tengan una herramienta que les facilite realizar dicha evaluación y medir el nivel de seguridad con que manejan la información. El **33.33%** de las instituciones realizaban evaluaciones al personal sobre la seguridad, y el **2.38%** dijeron que no sabían si les evaluaban.

- **Herramientas de seguridad**

Objetivo: Conocer si las instituciones cuentan con herramientas de seguridad para evaluar las bases de datos y redes informáticas.

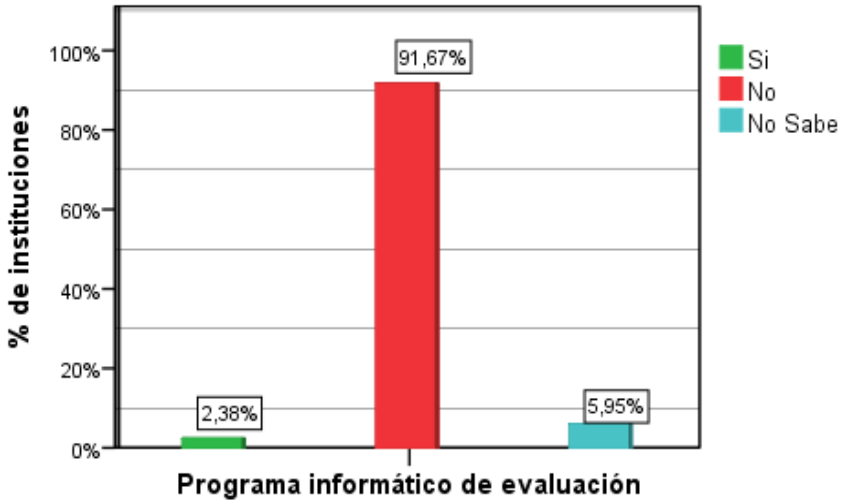
9-¿Cuentan localmente con un programa que les permita evaluar la seguridad de las bases de datos y redes informáticas? (No se consideran los antivirus).

Tabla 49: Cuenta con programa de evaluación de seguridad

Opciones	Frecuencia	Porcentaje
Si	2	2.4%
No	77	91.7%
No Sabe	5	6.0%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 40: Programa informático de evaluación de seguridad de la información



Fuente: Elaboración propia

Análisis:

Según los datos obtenidos la mayor parte de las instituciones encuestadas no contaban localmente con un programa que les permitiera evaluar o medir el nivel de seguridad en sus bases de datos y redes informáticas, el cual está representado en un **91.67%,** y un **5.95%** no sabían si lo tenían, por lo que no contaban específicamente con una herramienta que les facilitara la evaluación de sus datos. El contar con un programa de evaluación de seguridad representa muchos beneficios a las instituciones ya que les facilita la evaluación al personal y se ahorra tiempo en realizarla, de igual forma luego de haber realizado la evaluación se obtiene de forma veraz y oportuna un informe detallado del nivel de seguridad que presenta la información manejada digitalmente y así se sabe con certeza si se está fallando en algún área.

Variable dependiente: Nivel de seguridad en sus bases de datos y redes informáticas

Indicadores:

- **Incumplimiento de políticas**

Objetivo: Identificar si las instituciones están aplicando y utilizando políticas de seguridad informática.

13-¿Cuál de las siguientes afirmaciones describe mejor la condición de las políticas de seguridad informática en su lugar de trabajo?

Análisis:

En la mayoría de las instituciones no se contaba con políticas de seguridad informática, esta mayoría se ve representada por el **60.71%** de las instituciones, el **14.29%** afirmo que las políticas de su institución están en desarrollo, lo que indicaba que estas instituciones tampoco tenían políticas de seguridad informática, en el **7.14%** de las instituciones se contaba con políticas pero no se implementaban y únicamente en un **9.52%** de las instituciones se implementaban las políticas establecidas. La falta de políticas afectaba a la seguridad física ya que no se tenían establecidas las normas para guiar las actividades que pueden realizarse cotidianamente o en casos de riesgos (ver gráfica 14, pág. 91).

- **Falta de conocimientos**

Objetivo: Conocer si el personal que labora en las instituciones tiene conocimiento de algún programa informático para evaluar el nivel de seguridad de la información digital.

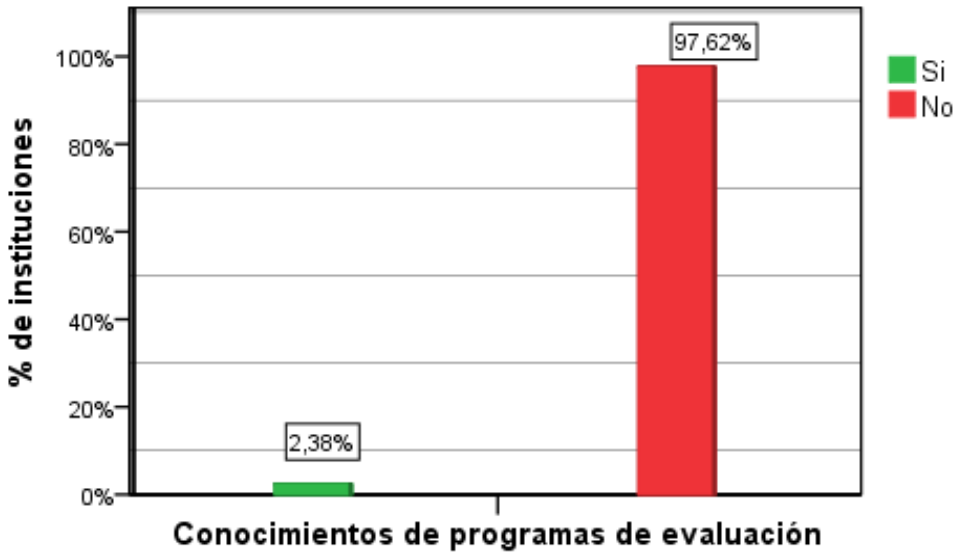
8-¿Conoce algún programa para evaluar el nivel de seguridad con que se maneja la información digital?

Tabla 50: Conocimiento de programas de evaluación de seguridad

Opciones	Frecuencia	Porcentaje
Si	2	2.4%
No	82	97.6%
Total	**84**	**100.0%**

Fuente: Elaboración propia

Gráfica 41: Conocimientos de programas de evaluación de seguridad informática



Fuente: Elaboración propia

Análisis:

La gráfica 41 refleja que casi en su totalidad el **97.62%** de las instituciones contaban con personal que desconocía de la existencia de algún programa informático que fuera útil para medir el nivel de seguridad de la información, por lo que concluimos que este tipo de programas o herramientas no eran muy conocidas por las instituciones, además de saber que las instituciones no están utilizando un programa de este tipo.

CAPÍTULO IV. PRUEBA DE HIPÓTESIS.

Síntesis

Se presenta la comprobación de las hipótesis planteadas, utilizando la prueba estadística ji cuadrado, para la cual se realiza una breve descripción y posteriormente se muestra la aplicación de la prueba estadística la interpretación de resultados y conclusiones además se determina la condición actual de la seguridad de las bases de datos y redes informáticas en el departamento de San Vicente.

4.1. DESCRIPCIÓN DE LA PRUEBA ESTADÍSTICA

El modelo utilizado para la comprobación de las hipótesis fue “la prueba de bondad de ajuste chi-cuadrada”, conocida también como “ji cuadrada”,

Fórmula utilizada:

$$X^2_{prueba} = \sum_{i=1}^{k} \frac{(o_1 - e_1)^2}{e_1}$$ (Monge y otros, (s. f.), p.5)

Dónde:

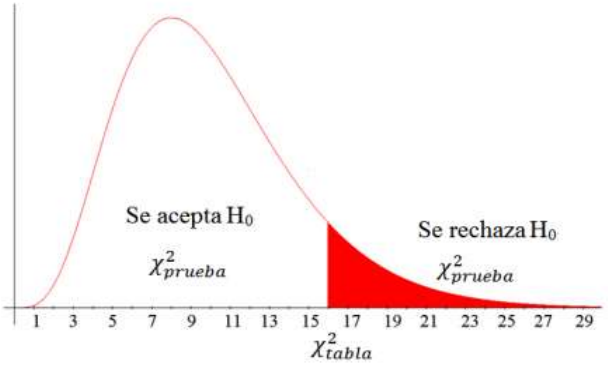
o_1: Es la frecuencia observada (la que se observa directamente en la muestra)

e_1: Es la frecuencia esperada (la que se calcula de acuerdo a las leyes de probabilidad).

La distribución ji cuadrada tiene una forma que depende del número de grados de libertad asociados a un determinado problema.

Para obtener un valor crítico (valor que deja un determinado porcentaje de área en la cola) a partir de una tabla de ji cuadrado, se debe seleccionar un nivel de significación y determinar los grados de libertad para el problema que se esté resolviendo.

La prueba ji cuadrado requiere la comparación del X^2_{Prueba} con el X^2_{tabla}. Si el valor estadístico de prueba es menor que el valor tabular, la hipótesis nula es aceptada, caso contrario, H0 es rechazada.



Nota: Un valor estadístico de X^2_{Prueba} menor que el valor crítico X^2_{tabla} o igual a él se considera como prueba de la variación casual en donde H0 es aceptada.

Descripción de los pasos para la prueba estadística:

1. Crear una tabla para ordenar las preguntas con su frecuencia observada y esperada, agrupándolas por indicador con su respectiva variable y luego asignar los valores de peso para cada pregunta dentro de los indicadores, los cuales deben cumplir el 100%

2. Calcular la media ponderada por variable y para cada indicador teniendo en cuenta el peso (%) de cada pregunta.

3. Sustituir las medias ponderadas de las frecuencias esperadas y observadas, en la fórmula de la prueba estadística ji cuadrada.

4. Calcular la ji cuadrada por medio de la tabla, teniendo el nivel de significancia y grados de libertad (ver anexo Nº 4, pág. 239).

5. Comparar ambos resultados y probar: si la x^2 calculada en el estadístico es mayor, que la calculada con la tabla, $x^2 > x^2(1-\alpha; m-k-1)$, queriendo decir que se rechaza la hipótesis nula, aceptando la de trabajo.

4.1.1. Justificación de la prueba estadística

La prueba de ji cuadrada es un cálculo que se utiliza para ver qué tanto se parece la distribución observada con los resultados teóricos, para determinar si un suceso es al azar o tiene alguna tendencia. Por lo tanto es la ji cuadrada la prueba estadística que se eligió para la comprobación de las hipótesis dado que se requería comprobar que los fenómenos estudiados marcaban una tendencia y no eran producidos al azar.

Esta prueba es útil en análisis de casos de una muestra, de dos muestras independientes, o en k muestras independientes, que involucran datos nominales. Típicamente es utilizada en casos donde los eventos, personas u objetos son agrupados en dos o más categorías nominales, tales como: "si-no", "a favor, en contra, indeciso", o clases A, B, C, D.

Es una prueba del tipo no paramétrica, las pruebas de este tipo son aquellas cuyo modelo no especifica condiciones sobre los parámetros de la población de donde se extrajo la muestra; es decir, el modelo no implica el uso de hipótesis que prefijen valor alguno de los parámetros poblacionales, sino que estas versan sobre características no numéricas.

4.2. APLICACIÓN DE LA PRUEBA ESTADÍSTICA

4.2.1. Prueba estadística de hipótesis 1

H1: Actualmente los usuarios que laboran en las instituciones no están capacitados adecuadamente en aspectos de seguridad sobre la información que manejan.

Ho1. Actualmente los usuarios que laboran en las instituciones están capacitados adecuadamente en aspectos de seguridad sobre la información que manejan.

Aplicación de la prueba estadística

1. Se creó una tabla para ordenar las preguntas con su frecuencia observada y esperada, agrupándolas por indicador con su respectiva variable y luego se asignaron los valores de peso para cada pregunta dentro de los indicadores, los cuales deben cumplir el 100%

   Fórmula para la frecuencia esperada:

$$fe = \frac{Conteo\ total}{Número\ de\ opciones}$$

Tabla 51: Cálculo de frecuencias con sus respectivos pesos por pregunta de la variable independiente

Variable Independiente	Indicadores	Preguntas	Opciones de respuesta	Frecuencias		Total de frecuencias		Peso por pregunta
				Observadas	Esperadas	Observadas	Esperadas	
Usuarios no capacitados	Recursos económicos	10-¿En el último año se ha invertido presupuesto en aspectos que contribuyan en la mejora de la seguridad de la información perteneciente a la institución donde labora?	Si	21	42	70	84	25%
			No	49	42			
		11-¿En su lugar de trabajo se asigna periódicamente parte del tiempo laboral, a capacitaciones sobre seguridad informática?	Si	16	42	70	84	75%
			No	54	42			

	Conocimientos de informática	12-¿Cada cuánto tiempo recibe cursos de actualización sobre seguridad informática?	Si	19	42	77	84	75%
			No	58	42			
		13 - ¿Cuál de las siguientes afirmaciones describe mejor la condición de las políticas de seguridad informática en su lugar de trabajo?	No se tienen políticas de seguridad definidas	51	21	77	84	25%
			Actualmente se encuentran en desarrollo	12	21			
			Política formal, no implementada	6	21			
			Política formal, escrita e informada al personal	8	21			

	Disponibilidad de tiempo	12-¿Cada cuánto tiempo recibe cursos de actualización sobre seguridad informática?	Anual	13	28	82	84	25%
			Semestral	6	28			
			No recibe	63	28			
		11-¿En su lugar de trabajo se asigna periódicamente parte del tiempo laboral, a capacitaciones sobre seguridad informática?	Si	19	42	82	84	75%
			No	63	42			

Fuente: Elaboración propia

Tabla 52: Cálculo de frecuencias con sus pesos por pregunta de la variable dependiente

Variable Dependiente	Indicadores	Preguntas	Opciones de respuesta	Frecuencias		Total de frecuencias		Peso por pregunta
				Observadas	Esperadas	Observadas	Esperadas	
Poca seguridad sobre la información que manejan.	Políticas de seguridad implementadas	13-¿Cuál de las siguientes afirmaciones describe mejor la condición de las políticas de seguridad informática en su lugar de trabajo?	Implementadas	10	42	71	84	75%
			No Implementadas	61	42			
		4-¿La asistencia técnica al equipo informático de su lugar de trabajo es	Si	10	42	71	84	25%
			No	61	42			

		proporcionada por?						
	Uso inadecuado de herramientas o equipo	14-¿Hace uso de las siguientes herramientas en su equipo de trabajo?	Si	37	42	81	84	75%
			No	44	42			
		19-¿Se ha enfrentado a alguna de las siguientes amenazas de seguridad de la información?	Si	70	42	81	84	25%
			No	11	42			

Fuente: Elaboración propia

2. Se calculó la media ponderada por variable y para cada indicador teniendo en cuenta el peso (%) de cada pregunta.

Tabla 53: Medias ponderadas de las frecuencias observadas

Variables	Indicadores	Peso por indicador (%)	Media ponderada por indicador	Media ponderada por variable
VI: Usuarios no capacitados	Recursos económicos	33.33%	70	76.33
	Conocimientos de informática	33.33%	77	
	Disponibilidad de tiempo	33.34%	82	
VD: Poca seguridad sobre la información que manejan	Políticas de seguridad implementadas	50%	71	76
	Uso inadecuado de Herramientas o equipo	50%	81	

Fuente: Elaboración propia

Tabla 54: Medias ponderadas de la frecuencia esperada

Variables	Indicadores	Peso por indicador (%)	Media ponderada por indicador	Media ponderada por variable
VI: Usuarios no capacitados	Recursos económicos	33.33%	84	84
	Conocimientos de informática	33.33%	84	
	Disponibilidad de tiempo	33.34%	84	
VD: Poca seguridad sobre la información que manejan.	Políticas de seguridad implementadas	50%	84	84
	Uso inadecuado de Herramientas o equipo	50%	84	

Fuente: Elaboración propia

Bondad de ajuste utilizando la ji cuadrada

3. Se sustituyeron las medias ponderadas de las frecuencias esperadas y observadas, en la fórmula de la prueba estadística ji cuadrada.

Fórmula de ji cuadrada:

$$X^2_{prueba} = \sum_{i=1}^{k} \frac{(o_1 - e_1)^2}{e_1}$$

Dónde: o = frecuencia observada en cada celda

e = frecuencia esperada en cada celda

Cálculo de la ji cuadrada:

$$X^2_{prueba} = \frac{(76.33-84)^2}{84} + \frac{(76-84)^2}{84}$$

$$\boldsymbol{X^2_{prueba}} = 0.7003 + 0.7619 = \mathbf{1.4622}$$

4. Se calculó la ji cuadrada por medio de la tabla, teniendo el nivel de significancia y grados de libertad (ver anexo Nº 4, pág. 239).

$$X^2_{(0.95,1)} = \mathbf{0.0039}$$

5. Se compararon ambos resultados para probar: si la x2 calculada en el estadístico es mayor, que la calculada con la tabla, x2 > x2 (1-α; m-k-1), queriendo decir que se rechaza la hipótesis nula, aceptando la de trabajo.

Comparando se tiene:

1.4622 > 0.0039

Interpretación

Este resultado indica que se rechaza la hipótesis nula y se acepta la hipótesis de trabajo: Actualmente los usuarios que laboran en las instituciones no están capacitados adecuadamente en aspectos de seguridad sobre la información que manejan.

4.2.2. Prueba estadística de hipótesis 2

H2. La pérdida de información de las instituciones se debe a la falta de aplicación de medidas de seguridad lógica.

Ho2. La pérdida de información de las instituciones no se debe a la falta de aplicación de medidas de seguridad lógica.

Aplicación de la prueba estadística

1. Se creó una tabla para ordenar las preguntas con su frecuencia observada y esperada, agrupándolas por indicador con su respectiva variable y luego se asignaron los valores de peso para cada pregunta dentro de los indicadores, los cuales deben cumplir el 100%

Tabla 55: Cálculo de frecuencias con sus respectivos pesos por pregunta de la variable independiente

Variable Independiente	Indicadores	Preguntas	Opciones de respuesta	Frecuencias		Total de frecuencias		Peso por pregunta
				Observadas	Esperadas	Observadas	Esperadas	
Falta de aplicación de medidas de seguridad lógica	Falta de conocimiento	15-Cuándo se realizan actualizaciones en el sistema informático ¿Se imparten las capacitaciones necesarias?	Si	26	42	73	84	75%
			No	47	42			
		4-¿La asistencia técnica al equipo informático de su lugar de trabajo es proporcionada por?	Si	10	42	73	84	25%
			No	63	42			
	Tipo de	16-La	Publica	7	28	82	84	50%

	información manejada	información que maneja en su lugar de trabajo es de carácter:	Privada	59	28			
			Ambos	16	28			
		7-¿En su lugar de trabajo le evalúan la seguridad con que maneja la información almacenada digitalmente?	Si	28	42	82	84	50%
			No	54	42			

Fuente: Elaboración propia

Tabla 56: Cálculo de frecuencias con sus respectivos pesos por pregunta de la variable dependiente

Variable Dependiente	Indicadores	Preguntas	Opciones de respuesta	Frecuencias		Total de frecuencias		Peso por pregunta
				Observadas	Esperadas	Observadas	Esperadas	
Pérdida de información de las instituciones	Contraseña	17-¿Utiliza contraseña para acceder a la información que almacena en su equipo de trabajo?	Si	68	42	84	84	50%
			No	16	42			
		16 La información que maneja en su lugar de trabajo es de carácter:	Pública	7	28	84	84	50%
			Privada	61	28			
			Ambos	16	28			
	Amenazas más comunes	19-¿Se ha enfrentado a alguna de las siguientes amenazas de seguridad de la información?	Si	70	42	81	84	75%
			No	11	42			

		(selección múltiple)						
		14¿Hace uso de las siguientes herramientas en su equipo de trabajo?	Si	37	42	81	84	25%
			No	44	42			
	Copias de seguridad	20-¿Cuáles de los siguientes medios utiliza actualmente la institución para almacenar las copias de seguridad?	Si	74	42	79	84	50%
			No	5	42			
		16-La información que maneja en su lugar de trabajo es de carácter:	Pública	6	28	79	84	50%
			Privada	60	28			
			Ambos	13	28			
	Antivirus	22-La versión del antivirus	Gratuita	30	28	67	84	75%

		utilizado en su lugar de trabajo es:	Pagada	34	28			
			No se cuenta con antivirus	3	28			
		19. ¿Se ha enfrentado a alguna de las siguientes amenazas de seguridad de la información?	Si	62	42	67	84	25%
			No	5	42			

Fuente: Elaboración propia

2. Se calculó la media ponderada por variable y para cada indicador teniendo en cuenta el peso (%) de cada pregunta.

Tabla 57: Medias ponderadas de las frecuencias observadas

Variables	Indicadores	Peso por indicador (%)	Media ponderada por indicador	Media ponderada por variable
VI: Falta de aplicación de medidas de seguridad lógica	Falta de conocimiento	50%	73	77.5
	Tipo de información manejada	50%	82	
VD: Pérdida de información de las instituciones.	Contraseña	25%	84	77.75
	Amenazas más comunes	25%	81	
	Copias de seguridad	25%	79	
	Antivirus	25%	67	

Fuente: Elaboración propia

Tabla 58: Medias ponderadas de la frecuencia esperada

Variables	Indicadores	Peso por indicador (%)	Media ponderada por indicador	Media ponderada por variable
VI: Falta de aplicación de medidas de seguridad lógica	Falta de conocimiento	50%	84	84
	Tipo de información manejada	50%	84	
VD: Pérdida de información de las instituciones.	Contraseña	25%	84	84
	Amenazas más comunes	25%	84	
	Copias de seguridad	25%	84	
	Antivirus	25%	84	

Fuente: Elaboración propia

Bondad de ajuste utilizando la ji cuadrada

3. Se sustituyeron las medias ponderadas de las frecuencias esperadas y observadas, en la fórmula de la prueba estadística ji cuadrada.

   Fórmula de ji cuadrada:

$$X^2_{prueba} = \sum_{i=1}^{k} \frac{(o_1 - e_1)^2}{e_1}$$

Dónde: o = frecuencia observada en cada celda

e = frecuencia esperada en cada celda

Cálculo de la ji cuadrada:

$$X^2_{prueba} = \frac{(77.5-84)^2}{84} + \frac{(77.75-84)^2}{84}$$

$$X^{\mathbf{2}}_{\boldsymbol{prueba}} = 0.5030 + 0.4650 = \mathbf{0.968}$$

4. Se calculó la ji cuadrada por medio de la tabla, teniendo el nivel de significancia y grados de libertad (ver anexo Nº 4, pág. 239).

$$X^2_{(0.95,1)} = \mathbf{0.0039}$$

5. Se compararon ambos resultados para probar: si la x2 calculada en el estadístico es mayor, que la calculada con la tabla, x2 > x2 (1-α; m-k-1), queriendo decir que se rechaza la hipótesis nula, aceptando la de trabajo.

Comparando se tiene:

0.968 > 0.0039

Interpretación

El resultado indico el rechazo de la hipótesis nula y la aceptación de la hipótesis de trabajo: La pérdida de información de las instituciones se debe a la falta de aplicación de medidas de seguridad lógica.

4.2.3. Prueba estadística de hipótesis 3

H3: Las instituciones no cuentan con un área informática interna que les brinde asistencia técnica inmediata.

Ho3. Las instituciones cuentan con un área informática interna que les brinde asistencia técnica inmediata.

.

Aplicación de la prueba estadística

1. Se creó una tabla para ordenar las preguntas con su frecuencia observada y esperada, agrupándolas por indicador con su respectiva variable y luego se asignaron los valores de peso para cada pregunta dentro de los indicadores, los cuales deben cumplir el 100%

Tabla 59: Cálculo de frecuencias con sus respectivos pesos por pregunta de la variable independiente

Variable Independiente	Indicadores	Preguntas	Opciones de respuesta	Frecuencias		Total de frecuencias		Peso por pregunta
				Observadas	Esperadas	Observadas	Esperadas	
VI: Falta de un área informática .	Falta de recursos económicos	2-¿En su lugar de trabajo se cuenta con los recursos económicos para la compra de equipo informático?	Si	25	42	80	84	50%
			No	55	42			
		1-¿En su lugar de trabajo cuentan con un departamento de informática interno?	Si	8	42	80	84	50%
			No	72	42			
	Asistencia técnica externa	4-¿La asistencia técnica al equipo informático de su lugar de trabajo es	Técnicos de sede central	39	21	77	84	75%
			Técnicos locales	10	21			
			Técnicos por	24	21			

		proporcionada por?	contrato temporal					
			No recibe asistencia	4	21			
		1-¿En su lugar de trabajo cuentan con un departamento de informática interno?	Si	7	42	77	84	25%
			No	70	42			

Fuente: Elaboración propia

Tabla 60: Cálculo de frecuencias con sus respectivos pesos por pregunta de la variable dependiente

Variable Dependiente	Indicadores	Preguntas	Opciones de respuesta	Frecuencias		Total de frecuencias		Peso por pregunta
				Observadas	Esperadas	Observadas	Esperadas	
VI: No se brinda asistencia técnica inmediata	Equipo adecuado	3-¿En su lugar de trabajo poseen herramientas para realizar el mantenimient	Si	13	42	79	84	25%
			No	66	42			

		o del equipo informático?						
		5-¿En caso de fallos en el equipo y/o en la red en cuanto tiempo aproximada mente recibe asistencia técnica?	Si	25	42	79	84	75%
			No	54	42			
	Personal no capacitado	4-¿La asistencia técnica al equipo informático de su lugar de trabajo es proporcionada por?	Si	10	42	77	84	50%
			No	67	42			
		12-¿Cada cuánto tiempo recibe cursos de actualización	Si	17	42	77	84	50%
			No	60	42			

		sobre seguridad informática?						
	Accesibilidad	5-¿En caso de fallos en el equipo y/o en la red en cuanto tiempo aproximadamente recibe asistencia técnica?	Inmediatamente	23	16.8	75	84	50%
			De 1 a 5 días	39	16.8			
			De 6 a 15 días	4	16.8			
			De 16 a 30 días	3	16.8			
			No recibe asistencia	6	16.8			
		4-¿La asistencia técnica al equipo informático de su lugar de trabajo es proporcionada por?	Si	10	42	75	84	50%
			No	65	42			

Fuente: Elaboración propia

2. Se calculó la media ponderada por variable y para cada indicador teniendo en cuenta el peso (%) de cada pregunta.

Tabla 61: Medias ponderadas de las frecuencias observadas

Variables	Indicadores	Peso por indicador (%)	Media ponderada por indicador	Media ponderada por variable
VI: Falta de un área informática	Falta de recursos económicos	50%	80	78.5
	Asistencia técnica	50%	77	
VD: No se brinda asistencia técnica inmediata	Equipo adecuado	33.33%	79	77
	Personal no capacitado	33.33%	77	
	Accesibilidad	33.34%	75	

Fuente: Elaboración propia

Tabla 62: Medias ponderadas de la frecuencia esperada

Variables	Indicadores	Peso por indicador (%)	Media ponderada por indicador	Media ponderada por variable
VI: Falta de un área informática	Falta de recursos económicos	50%	84	84
	Asistencia técnica	50%	84	
VD: No se brinda asistencia técnica inmediata	Equipo adecuado	33.33%	84	84
	Personal no capacitado	33.33%	84	
	Accesibilidad	33.34%	84	

Fuente: Elaboración propia

Bondad de ajuste utilizando la ji cuadrada

3. Se sustituyeron las medias ponderadas de las frecuencias esperadas y observadas, en la fórmula de la prueba estadística ji cuadrada.

Fórmula de ji cuadrada:

$$X^2_{prueba} = \sum_{i=1}^{k} \frac{(o_1 - e_1)^2}{e_1}$$

Dónde: o = frecuencia observada en cada celda

e = frecuencia esperada en cada celda

Cálculo de la ji cuadrada:

$$X^2_{prueba} = \frac{(78.5-84)^2}{84} + \frac{(77-84)^2}{84}$$

$$X^2_{prueba} = 0.3601 + 0.5833 = \mathbf{0.9434}$$

4. Se calculó la ji cuadrada por medio de la tabla, teniendo el nivel de significancia y grados de libertad (ver anexo Nº 4, pág. 239).

$$X^2_{(0.95,1)} = \mathbf{0.0039}$$

5. Se compararon ambos resultados para probar: si la x2 calculada en el estadístico es mayor, que la calculada con la tabla, x2 > x2 (1-α; m-k-1), queriendo decir que se rechaza la hipótesis nula, aceptando la de trabajo.

Comparando se tiene:

0.9434 > 0.0039

Interpretación

Se obtuvo como resultado el rechazo de la hipótesis nula y la aceptación de la hipótesis de trabajo: Las instituciones no cuentan con un área informática interna que les brinde asistencia técnica inmediata.

4.2.4. Prueba estadística de hipótesis 4

H4. El equipo informático de las instituciones públicas, privadas y no gubernamentales se encuentra expuesto a riesgos físicos.

Ho4. El equipo informático de las instituciones públicas, privadas y no gubernamentales no se encuentra expuesto a riesgos físicos.

Aplicación de la prueba estadística

1. Se creó una tabla para ordenar las preguntas con su frecuencia observada y esperada, agrupándolas por indicador con su respectiva variable y luego se asignaron los valores de peso para cada pregunta dentro de los indicadores, los cuales deben cumplir el 100%.

Tabla 63: Cálculo de frecuencias con sus respectivos pesos por pregunta de la variable independiente

Variable Independiente	Indicadores	Preguntas	Opciones de respuesta	Frecuencias		Total de frecuencias		Peso por pregunta
				Observadas	Esperadas	Observadas	Esperadas	
VI: Riesgos físicos.	Infraestructura	23-¿Seleccione los problemas de infraestructura que representan riesgo para los equipos que almacenan la información en su lugar de trabajo? (selección múltiple)	Si	59	42	79	84	75%
			No	20	42			
		29-¿Cuál de las siguientes razones ha afectado el buen funcionamiento de su equipo informático? (selección múltiple)	Si	68	42	79	84	25%
			No	11	42			
	Sobrecalentamiento del equipo	24-¿El equipo Informático en que trabaja ha presentado problemas de sobrecalentamiento?	Si	58	42	80	84	50%
			No	22	42			

		29-¿Cuál de las siguientes razones ha afectado el buen funcionamiento de su equipo informático? (selección múltiple)	Si	31	42	80	84	50%
			No	49	42			
	Delincuencia	25-¿En su lugar de trabajo se han presentado casos de robo de equipo informático?	Si	8	42	81	84	
			No	73	42			
		30-¿El equipo informático que almacena la información se encuentra expuesto a la afluencia de personas ajenas a la institución donde labora?	Si	10	42	81	84	
			No	71	42			

Fuente: Elaboración propia

Tabla 64: Cálculo de frecuencias con sus respectivos pesos por pregunta de la variable dependiente

Variable Dependiente	Indicadores	Preguntas	Opciones de respuesta	Frecuencias		Total de frecuencias		Peso por pregunta
				Observadas	Esperadas	Observadas	Esperadas	
Vulnerabilidad del equipo informático.	Vida útil	26-¿Aproximadamente cuánto tiempo tiene de uso la computadora en que trabaja?	Menos de 1 año	12	21	84	84	100%
			De 1 a 2 años	21	21			
			De 3 a 5 años	28				
			Más de 5 años	23				
	Acondicionamiento	29-¿Cuál de las siguientes razones ha afectado el buen funcionamiento de su equipo informático? (selección múltiple)	Si	62	42	84	84	50%
			No	22	42			

		31-¿Su equipo informático ha presentado alguno de los siguientes fallos de rendimiento? (selección múltiple)	Si	64	42	84	84	50%
			No	20	42			
	Ubicación	23- ¿Seleccione los problemas de infraestructura que representan riesgo para los equipos que almacenan la información en su lugar de trabajo? (selección múltiple)	Si	43	42	79	84	100%
			No	36	42			

	Capacidad	31-¿Su equipo informático ha presentado alguno de los siguientes fallos de rendimiento? (selección múltiple)	Si	64	42	84	84	50%
			No	20	42			
		26- ¿Aproximadamente cuánto tiempo tiene de uso la computadora en que trabaja?	Menos de 1 año	12	21	84	84	50%
			De 1 a 2 años	21	21			
			De 3 a 5 años	28	21			
			Más de 5 años	23	21			

	Mantenimiento al equipo	32-¿Qué tipo de mantenimiento se realiza en el equipo informático de su lugar de trabajo? (selección múltiple)	Si	40	42	84	84	50%
			No	44	42			
		31-¿Su equipo informático ha presentado alguno de los siguientes fallos de rendimiento? (selección múltiple)	Si	64	42	84	84	50%
			No	20	42			

Fuente: Elaboración propia

2. Se calculó la media ponderada por variable y para cada indicador teniendo en cuenta el peso (%) de cada pregunta.

Tabla 65: Medias ponderadas de las frecuencias observadas

Variables	Indicadores	Peso por indicador	Media ponderada por	Media ponderada
VI: Riesgos físicos	Infraestructura	33.33%	79	80
	Sobrecalentamiento del equipo	33.33%	80	
	Delincuencia	33.34%	81	
VD: Vulnerabilidad del equipo informático	Vida útil	20%	84	83
	Acondicionamiento	20%	84	
	Ubicación	20%	79	
	Capacidad	20%	84	
	Mantenimiento al equipo	20%	84	

Fuente: Elaboración propia

Tabla 66: Medias ponderadas de la frecuencia esperada

Variables	Indicadores	Peso por indicador (%)	Media ponderada por indicador	Media ponderada por variable
VI: Riesgos físicos	Infraestructura	33.33%	84	84
	Sobrecalentamiento del equipo	33.33%	84	
	Delincuencia	33.34%	84	
VD: Vulnerabilidad del equipo informático	Vida útil	20%	84	84
	Acondicionamiento	20%	84	
	Ubicación	20%		
	Capacidad	20%	84	
	Mantenimiento al equipo	20%	84	

Fuente: Elaboración propia

Bondad de ajuste utilizando la ji cuadrada

3. Se sustituyeron las medias ponderadas de las frecuencias esperadas y observadas, en la fórmula de la prueba estadística ji cuadrada.

   Fórmula de ji cuadrada:

$$X^2_{prueba} = \sum_{i=1}^{k} \frac{(o_1 - e_1)^2}{e_1}$$

Dónde: o = frecuencia observada en cada celda

e = frecuencia esperada en cada celda

Cálculo de la ji cuadrada:

$$X^2_{prueba} = \frac{(80-84)^2}{84} + \frac{(83-84)^2}{84}$$

$$X^2_{\boldsymbol{prueba}} = 0.1905 + 0.0119 = \mathbf{0.2024}$$

4. Se calculó la ji cuadrada por medio de la tabla, teniendo el nivel de significancia y grados de libertad (ver anexo Nº 4, pág.239).

$$X^2_{(0.95,1)} = \mathbf{0.0039}$$

5. Se compararon ambos resultados para probar: si la x2 calculada en el estadístico es mayor, que la calculada con la tabla, x2 > x2 (1-α; m-k-1), queriendo decir que se rechaza la hipótesis nula, aceptando la de trabajo.

Comparando se tiene:

0.2024 > 0.0039

Interpretación

Se obtuvo como resultado el rechazo de la hipótesis nula y la aceptación de la hipótesis de trabajo: El equipo informático de las instituciones públicas, privadas y no gubernamentales se encuentra expuesto a riesgos físicos.

4.3. CONCLUSIONES DE LOS RESULTADOS OBTENIDOS

Hipótesis general

Con el análisis realizado utilizando la prueba estadística ji cuadrada se pudo determinar la aceptación de la hipótesis general por medio de la comprobación de las hipótesis específicas o de trabajo planteadas en nuestra investigación, por lo tanto se puede afirmar que en la actualidad, las instituciones públicas, privadas y no gubernamentales del departamento de San Vicente, tienen la necesidad de una herramienta informática de evaluación que les permitan determinar el nivel de seguridad en sus bases de datos y redes informáticas.

Ya que los datos proporcionados por la investigación demostraron que en la mayoría de las instituciones no se estaban brindando las capacitaciones necesarias para mantener al personal actualizado, de tal manera que tenga la capacidad de proporcionar las barreras de seguridad adecuadas e identificar si en algún momento se estaban presentando vulnerabilidades en la seguridad, debido a que en su mayoría las instituciones limitaban a su personal únicamente a tareas mecánicas y no era una prioridad para ellas actualizar los conocimientos de sus empleados de manera constante para que pudieran reaccionar de la mejor manera ante problemas que pongan en riesgo la seguridad de la información que manejan. Por lo tanto una herramienta que les permita a las instituciones evaluar el nivel de seguridad con que se está manejando la información, seria de mucha utilidad para reforzar esta deficiencia ya que les permite a los usuarios concientizarse de las debilidades de seguridad informática a las que están expuestos.

También en las instituciones se identificaron algunos problemas de seguridad lógica por omitir medidas de seguridad básicas tales como acceder a páginas de descarga en horas

laborales, no utilizar contraseñas o no cambiar las contraseñas periódicamente, como también se evadían medidas de seguridad física que ponían en riesgo la seguridad del equipo que resguarda la información de las instituciones, agregado a esto se encontró la falta de un área de informática que les brindara asistencia técnica inmediata y que además fuera la responsable de analizar las debilidades de la seguridad en la información digital y solventar los problemas lógicos y físicos que podrían estarse dando, en estos casos una herramienta que ayude a identificar los problemas de seguridad a los que se enfrenta la información digital serviría de mucho apoyo a las instituciones del departamento de San Vicente.

A continuación se describirán más a profundidad los resultados obtenidos para las hipótesis de trabajo tomando en consideración los indicadores de las hipótesis.

Hipótesis 1

La mayoría de las instituciones del departamento de San Vicente no estaban capacitando a sus empleados periódicamente en aspectos que contribuyeran a la seguridad de la información digital, esto se pudo afirmar considerando el análisis realizado, tomando en cuenta varios indicadores que influyen en el problema de falta de capacitación, considerando el análisis estadístico realizado, puede afirmarse que los recursos económicos eran uno de los factores que afectaban la falta de capacitación ya que las instituciones que no habían invertido presupuesto en aspectos de seguridad informática tampoco habían asignado tiempo a capacitar a su personal, presentando un índice alto de falta de capacitación, la incidencia de este elemento en la falta de capacitación se comprobó por medio de la relación estadística de estos dos elementos además el recurso económico es indispensable para poder efectuar capacitaciones ya que estas implican gastos en pago a especialistas que capaciten y tiempo laboral que no producirá utilidades inmediatamente por lo que no pueden realizarse capacitaciones sin presupuesto asignado para esto. Otro factor que se identificó como influyente en la falta de capacitación al personal fue la falta de implementación de políticas presentándose en la mayoría de los casos la falta de capacitación en las instituciones que no habían implementado políticas de seguridad informática, identificando el hecho que las instituciones no tuvieran un conjunto de normas de seguridad que les brinde una guía de las cosas que debían o no debían hacerse como un motivo para brindar menor importancia al hecho de mantener capacitado

a su personal. Además se identificaron una serie de problemas relacionados con la falta de capacitación al personal ya que se estaban descuidando aspectos muy importantes pero de aplicación simple como eran el evitar descargas en equipos de trabajo laboral, cambiar las contraseñas periódicamente o no ingerir alimentos cerca del equipo informático, estos problemas no se presentaron con tanta frecuencia en instituciones que instruían correctamente a su personal sobre la seguridad informática.

Al ser la falta de recursos económicos, la falta de políticas y la falta de tiempo algunos de los indicadores que influyen en la ausencia de capacitaciones, se puede afirmar que las instituciones tienen la necesidad de obtener una herramienta que les guie para que puedan identificar el nivel de seguridad con que están trabajando y cuáles son sus deficiencias para poder superarlas, por lo tanto seria de mucha utilidad la implementación de una herramienta gratuita que ayude a identificar los niveles de seguridad con los que se está manejando la información en las instituciones del departamento de San Vicente, la herramienta haría un sondeo de las áreas que están teniendo deficiencia de seguridad informática y además no se necesitaría de mucho tiempo para realizar una evaluación con el software.

Hipótesis 2

La pérdida de información de las instituciones se producía en muchos casos debido a la falta de aplicación de medidas de seguridad lógica. El personal encargado del registro de la información no ponía en práctica ciertos aspectos de seguridad porque no conocía las medidas que podrían contribuir a superarlos, los principales problemas identificados por medio de la investigación fueron: uso inapropiado de contraseñas para el manejo de información pública como privada, el uso de herramientas de descargas en equipos que se utilizan para almacenar información institucional, el manejo incorrecto o la no realización de respaldos de información y la infiltración de virus. En cuanto a la creación de respaldos de la información manejada por las instituciones, en la mayoría de los casos se utilizaban memorias USB como único medio de almacenamiento de respaldos o como mecanismo de almacenamiento alternativo a los discos duros, cabe mencionar que este no es un medio apropiado para almacenar respaldos de información importante ya que estos dispositivos

pueden ser hurtados, olvidados o perdidos con facilidad lo que expone la información almacenada en ellos, además la falta de evaluación de la seguridad de la información manejada tanto en instituciones públicas, privadas y no gubernamentales es un factor de mucha incidencia al problema de inseguridad de la información ya que si no se utilizan mecanismos de evaluación no se tiene conciencia de los problemas de inseguridad de la información a los que se está expuesto pudiendo tener muchas deficiencias y no tener el conocimiento de estas para poder tratarlas, además la utilización del equipo informático de manera inadecuada es otro problema que se ha identificado en las instituciones del departamento de San Vicente ya que en un gran porcentaje estaban utilizando el equipo informático para actividades que no eran de carácter laboral como el acceso a redes sociales y páginas de descarga, como también estaban utilizando programas como ares, atube catcher, emule, entre otros que tienen la característica de ser un medio por el cual se pueden contraer virus de la red, considerando también que un buen porcentaje de instituciones estaban utilizando versiones de antivirus gratuitas lo que indica que los antivirus utilizados no son tan completos como una versión pagada, tomando en cuenta también que un antivirus gratuito es una versión de prueba que caduca en periodos de tiempo cortos, es probable que el antivirus sobrepase el tiempo de prueba y las computadoras se queden sin protección durante algún periodo, además de estos problemas también las instituciones han expresado por medio de las encuestas que se han enfrentado a virus, alteración de datos, robo de información, intrusos informáticos y hurto de contraseña.

Considerando los problemas de seguridad lógica que se identificaron en las instituciones de San Vicente, es recomendable la aplicación de una herramienta que les permita a las instituciones identificar cuáles son las debilidades de seguridad lógica a las que se están enfrentando y además que les ofrezca las alternativas de solución para poder reforzar la seguridad lógica y así poder evitar que se materialicen los riesgos que pueden afectar la integridad de la información.

Hipótesis 3

Las instituciones públicas, privadas y no gubernamentales del departamento de San Vicente no contaban con un área informática interna que les brindara asistencia técnica inmediata, una de las razones por las que esto se producía era debido a que no se asignaba el presupuesto necesario para ello por varios motivos, entre ellos estaban: las instituciones recibían asistencia de técnicos de sedes centrales, contrataban a técnicos externos cuando era necesario y en algunas instituciones se afirmó que no recibían asistencia técnica de ningún tipo, estos eran elementos que influían en la falta de un área de informática interno.

Por medio del análisis estadístico se pudo comprobar que son pocas las instituciones que recibían asistencia técnica local por lo tanto la gran mayoría no tenían especialistas internamente que brindaran asistencia técnica de forma inmediata o mantenimiento rutinario al equipo por consiguiente no se contaba con personal interno encargado de velar por la seguridad de la información de las instituciones ni monitorear constantemente las vulnerabilidades de seguridad informática que las instituciones tienen.

Tomando en cuenta estos problemas y la ausencia de especialistas informáticos en las instituciones, una herramienta de evaluación de la seguridad informática que sea de fácil aplicación y con medidas de seguridad que se adapten a las necesidades de diferentes instituciones y permita ofrecer soluciones de forma rápida y practica a problemas de seguridad que afectan a las bases de datos que contienen la información valiosa de las instituciones, cubriría muchas necesidades que presentan dichas instituciones para garantizar un buen nivel de seguridad para la información que manejan.

Hipótesis 4

Las instituciones presentaban vulnerabilidades físicos que podían afectar el buen funcionamiento del equipo informático entre algunas de estas vulnerabilidades se pueden mencionar el espacio reducido para la ubicación del equipo, la mala ubicación de los tomacorrientes, la ventilación inapropiada, la falta de limpieza rutinaria entre otras, encontrando una relación significativa entre los problemas de sobrecalentamiento del

equipo y las siguientes dos razones la ventilación inapropiada y la falta de limpieza rutinaria, además el equipo informático utilizado en la mayoría de las instituciones había sobrepasado el tiempo de vida útil, presentando en estos casos fallos en el equipo como apagones repentinos, congelamiento de pantallas y lentitud, además se identificó que las instituciones no aplicaban una buena ubicación en la organización de su equipo informático, que les permitiera optimizar el espacio y mejorar la seguridad de este, entre algunos de los problemas de seguridad física que fueron identificados por medio de la observación directa se pueden mencionar: una mala organización del cableado de red, la organización inadecuada de los cables de suministro eléctrico, la mala ubicación de los tomacorrientes donde cabe mencionar el caso de instalaciones eléctricas colocadas en el piso lo cual generaba riesgos al equipo, mayores probabilidades de deterioro para las instalaciones ya que debido al efecto de la gravedad el polvo y otras partículas tienden a alojarse en los orificios de los tomacorrientes, existiendo también una mayor vulnerabilidad hacia la humedad ya sea por desinfectantes aplicados al piso o por líquidos derramados accidentalmente, este tipo de instalaciones ubicadas en el piso también pueden complicar las condiciones en caso de desastres naturales como inundaciones ya que el agua es un buen conductor de la energía eléctrica y una pequeña inundación puede convertir al local en un campo eléctrico, con respecto a la mala ubicación de los muebles y el equipo se pudieron observar casos de acumulación de documentos que parecían no haber sido utilizados hace mucho tiempo que deberían estar ubicados en bodega o en sitios más aislados, ubicación de archiveros en lugares accesibles para las personas que ingresan a las instalaciones entre otros, También es considerado como un problema físico que afecta a las instituciones del departamento San Vicente la capacidad del hardware de las computadoras utilizadas ya que en la mayoría de las instituciones se utilizaban computadoras que ya habían excedido la vida útil en su mayoría con vidas mayores de 3 y 5 años.

Dejando demostrado que las instituciones del departamento de San Vicente presentaron problemas de seguridad física que representaban amenazas latentes para los equipos informáticos que a su vez afectaban la seguridad de la información, por lo tanto es necesario que dichas instituciones tengan una herramienta que les oriente sobre el nivel de seguridad física que están proporcionando a la información resguardada en sus equipos ya

que el daño físico que pueda ocasionársele al equipo afecta de manera directa a la información almacenada en él.

4.4. INTERPRETACIÓN DE RESULTADOS DE LA PRUEBA DE ESTADÍSTICA.

4.4.1. Determinación de la condición actual.

Determinación de criterios

Para poder establecer los criterios con los cuales determinaremos el nivel de seguridad de bases de datos y redes informáticas de las instituciones públicas, empresas privadas y no gubernamentales del departamento de San Vicente lo primero que se determinó fueron sus puntos vulnerables donde las amenazas eran más latentes, y las diferentes fortalezas que las instituciones tenían. Dicho análisis se dividió en dos áreas que fueron:

- Seguridad física
- Seguridad lógica

La identificación de las diversas vulnerabilidades y fortaleza en dichas áreas, se llevó a cabo por medio de las preguntas realizadas en las encuestas tanto de la etapa de anteproyecto como de diagnóstico.

La seguridad física y seguridad lógica a su vez se dividieron en dos partes:

- **Aspectos positivos**

En donde la respuesta “si” representa una fortaleza para la seguridad de la información.

- **Aspectos negativos**

En donde la respuesta “si” representa una amenaza para la seguridad de la información y cada parte está compuesta por diversos indicadores divididos en dos opciones donde su porcentaje en la opción “Si” y “No” representan el número de instituciones que ha sido afectada por dichas vulnerabilidades o que poseen dicha fortaleza.

Lo cual sirve como punto de partida para la determinación de un diagnóstico del nivel de seguridad, el propósito de realizar dicho diagnóstico es el identificar los huecos de seguridad que poseen las diferentes instituciones del departamento de San Vicente, que le permita tomar decisiones preventivas y correctivas para disminuir vulnerabilidades.

Finalidad de los niveles de seguridad determinados.

1.- Nivel de seguridad alto

La seguridad de alto nivel persigue reducir al mínimo posible, los elementos que puedan amenazar la confidencialidad, integridad y disponibilidad de la información. Para ello se centra en un número de elementos, con los que se es más estricto. La seguridad de alto nivel está orientada al trabajo con servidores y redes de comunicación. Es fundamental tomar las decisiones técnicas que más convengan a las necesidades de la red con la que estemos trabajando, tanto a nivel de hardware como de software.

En este nivel siempre existe cierto nivel de amenaza para la información y los sistemas aunque muy bajo. No obstante, los procedimientos de trabajo, vigilancias habituales, políticas y procedimientos planteados con anterioridad y evaluados de forma periódica, son eficaces.

2.- Nivel de seguridad medio

En este Nivel los riesgos y amenazas son emergentes, aunque sin confirmar, hacen necesaria la mejora de las medidas de prevención y protección tomadas, revisando y actualizando los procedimientos actuales de seguridad informática.

3.- Nivel de seguridad bajo

En este nivel existen amenazas que podrían tener un impacto significativo en la información. Además los responsables de seguridad deben incrementar la vigilancia, evaluar si las características del riesgo requieren del perfeccionamiento de algún procedimiento o de la implantación de alguna medida añadida e informar a los grupos de respuesta.

A. Seguridad física

Tabla 67: Niveles de seguridad física

N°	Aspecto de seguridad considerado	Frecuencia		Aspectos de seguridad	Criterio de evaluación	Nivel de seguridad
		Si	No			
Si = Fortaleza			**No = Vulnerabilidad**			
				Importancia		
1	Uso de UPS	53%	**47%**	Es bastante útil para realizar un proceso correcto de finalización de actividades de manejo de la información en un equipo informático, ya que brinda un lapso de tiempo extra para poder guardar cambios en casos de cortes eléctricos, además de regular la energía y suprimir los cambios de voltaje.	Considerando que la ausencia de UPS, alarmas de ingreso y aire acondicionado no es una vulnerabilidad que afecte directamente la información sino solo medios de prevención para evitar daños en el equipo en el que se registra o resguarda la información el criterio de evaluación considerado es el siguiente: Si el número de instituciones que posee dicha vulnerabilidad es:	Bajo
2	Uso de alarmas de ingreso	37%	**63%**	Advierten sobre alguna situación anormal de acceso no autorizado que ponga en riesgo el equipo que almacena la información		Bajo
3	Aire acondicionado donde	51%	**43%**	Para mantener el equipo		Bajo

	está ubicado el equipo informático que resguarda la información.			informático en el que se registran y almacenan los datos de la empresa, la temperatura apropiada para un buen estado del equipo ronda los 22º.	◆ Mayor de 40% = **Nivel de seguridad bajo** ◆ Entre 15% y 40% = **Nivel de seguridad medio** ◆ Menor al 15% = **Nivel de seguridad alto**	
4	Mantenimiento preventivo al equipo.	48%	**52%**	El mantenimiento preventivo evita los fallos en el equipo antes de que estos ocurran.	Si el número de instituciones que posee dicha vulnerabilidad es: ◆ Mayor de 50% = **Nivel de seguridad bajo** ◆ Entre 20% y 50% = **Nivel de seguridad medio** ◆ Menor al 20% = **Nivel de seguridad alto**	Bajo
5	Asignación de recursos económicos para la compra de equipo informático	30%	**65%**	Debido a que los equipos en los que se resguarda y registra la información se dañan al transcurrir del tiempo siempre se hace necesaria la asignación de presupuesto para que este equipo sea reemplazo y así garantizar que el manejo de la información se hará de una manera más eficiente.	Si el número de instituciones que posee dicha vulnerabilidad es: ◆ Mayor 60% = **Nivel de seguridad bajo** ◆ Entre 20% y 60% = **Nivel de seguridad medio** ◆ Menor al 20% = **Nivel de seguridad alto**	Bajo

Si = Vulnerabilidad					No = Fortaleza	
				Impacto		
6	Consumo de alimentos o bebidas mientras se trabaja en la computadora	**23%**	77%	Si llegase a derramarse alimentos o bebidas sobre el equipo informático se pueden dañar los componentes internos o provocar una falla eléctrica en el equipo**.**	Si el número de instituciones que posee dicha vulnerabilidad es: ◆ Mayor 50% = **Nivel de seguridad bajo** ◆ Entre 20% y 50% = **Nivel de seguridad medio** ◆ Menor al 20% = **Nivel de seguridad alto**	Medio
7	problemas de tomacorrientes insuficientes	**27%**	73%	Sobrecargar los tomacorrientes con conexiones en enchufes múltiples o saturarlos con accesorios, incrementa el riesgo de accidentes eléctricos y cortocircuitos	Estos problemas son problemas de infraestructura que no afectan en si a la información directamente si no las condiciones en las que la información se maneja, es por ello que su grado de importancia es bajo. Si el número de instituciones que posee dicha vulnerabilidad es:	Medio

					◆ Mayor 60% = **Nivel de seguridad bajo** ◆ Entre 20% y 60% = **Nivel de seguridad medio** ◆ Menor al 20% = **Nivel de seguridad alto**	
8	Computadoras con tiempo de uso mayor de dos año	**60%**	39%	Los equipos tienen una duración limitada. Procurar alargar al máximo de tiempo posible de uso puede volver al equipo vulnerable ya que se está mayormente propenso a fallos.	Estos problemas muestran las condiciones en las que se encuentra los equipo en el que se registra la información, esta problemática aunque sigue siendo indirecta esta aun poco más relacionada al manejo de la información: Si el número de instituciones que posee dicha vulnerabilidad es: ◆ Mayor 50% = **Nivel de seguridad bajo** ◆ Entre 20% y 50% = **Nivel de seguridad medio**	Bajo
9	Problemas de sobrecalentamiento en el equipo Informático	**37%**	57%	El sobrecalentamiento puede dañar los circuitos y chips de las computadoras.		Medio
10	Falta de limpieza rutinaria en el equipo informático	**65%**	34%	La falta de limpieza produce acumulación de suciedad, polvos y sustancias que puede provocar un mal funcionamiento de la PC y problemas como cortocircuitos, calentamientos, bloqueos y ruidos.		Bajo

11	Problemas de lentitud en equipo informático	**64%**	36%	La lentitud de respuesta de una computadora es muy molesta además representa un problema latente, al cual se le debe de prestar importante atención.	◆ Menor al 20% = **Nivel de seguridad alto.**	Bajo
12	equipo informático que almacena la información está expuesto a la Afluencia de personas ajenas a la institución	**12%**	88%	La información importante almacenada en los equipos es susceptible a robo, por lo tanto se deben tomar medidas respecto a las personas que acceden al lugar.	La afluencia de personas afecta en mayor medida si se trata de los equipos servidores, al no tratarse de estos afectaría solo indirectamente. Si el número de instituciones que posee dicha vulnerabilidad es: ◆ Mayor 50% = **Nivel de seguridad bajo** ◆ Entre 10% y 50% = **Nivel de seguridad medio** ◆ Menor al 10% = **Nivel de seguridad alto**	Medio

Fuente: Elaboración propia[1]

[1] Ver anexo Nº 6, pág. 260

B. Seguridad Lógica

Tabla 68: Niveles de seguridad lógica

N°	Aspecto de seguridad considerado	Frecuencia		Aspectos de seguridad	Criterio de evaluación	Nivel de seguridad
		Si	No			
Si= Fortaleza				**No= Vulnerabilidad**		
				Importancia		
1	Departamento de informática interno	11%	**89%**	Es el departamento donde se lleva a cabo la planeación, organización, dirección y control de las operaciones informáticas, con el objeto de asegurar la protección y disponibilidad de todos los recursos informáticos especialmente la información	Si el número de instituciones que posee dicha vulnerabilidad es: ◆ Mayor 60% = **Nivel de seguridad bajo** ◆ Entre 20% y 60% = **Nivel de seguridad medio** ◆ Menor al 20% = **Nivel de seguridad alto**	**Bajo**
2	Uso de un sistema informático para almacenar la información que manejan	100%	**0%**	La utilización de un sistema informático permite el acceso rápido a la información, permite la generación de informes e indicadores para corregir fallas y toma de decisiones, entre otros.		**Alto**

3	Sistema informático en red	90%	**10%**	Las redes informáticas son importantes ya que la información está disponible en muchas fuentes además que permite transportarla a gran velocidad y en grandes distancias.		**Alto**
4	Antivirus en las computadoras	86%	**11%**	La función de un programa antivirus es detectar y evitar, la presencia o el accionar de un virus informático que ponga en riesgo la información almacenada en una computadora.	El uso de antivirus, el uso de contraseña y la asistencia técnica inmediata en caso de fallo y las copias de seguridad involucran directamente la seguridad la información, es por ello que se consideran aspectos de mayor importancia: ◆ Mayor 30% = **Nivel de seguridad bajo** ◆ Entre 10% y 30% = **Nivel de seguridad medio** ◆ Menor al 10% = **Nivel de seguridad alto**	**Medio**
5	Uso de contraseña para acceder a la información	85%	**15%**	La definición de contraseñas seguras reduce los riesgos al acceso no autorizado, manipulación y destrucción de información de forma accidental o deliberada y la protege de una posible divulgación no autorizada.		**Medio**

6	Asistencia técnica inmediata en caso de fallos en el equipo y/o en la red.	30%	**70%**	La asistencia técnica inmediata permite mantener los equipos de computación que resguardan y registran la información en óptimo funcionamiento.		**Bajo**
7	Realización de copias de seguridad de la información que maneja	64%	**34%**	Un backup asegura la disposición de la información ante eventualidades tales como: Un fallo de software o de programación, daños de hardware, daños por virus, gusanos o ataques cibernéticos y catástrofes imprevisibles como incendios, robos si se mantienen en lugares diferentes a las instalaciones de trabajo.		**Bajo**
8	Almacenamiento de copias de seguridad fuera de los locales de trabajo	24%	**68%**			**Bajo**
9	Inversión de presupuesto en los últimos dos años en la compra de programas informáticos actualizados	45%	**46%**	Es fundamental mantener actualizaciones de aquellos programas tales como firewall, antivirus y otros que su des actualización puedan implicar un agujero de seguridad en caso de ser explotados por un	Estos aspectos involucran la seguridad de la información de manera indirecta por lo tanto su importancia es menor: Si el número de instituciones que posee dicha vulnerabilidad	**Medio**

				atacante o cualquier tipo de malware.	es: ◆ Mayor 50% = **Nivel de seguridad bajo** ◆ Entre 20% y 50% = **Nivel de seguridad medio** ◆ Menor al 20% = **Nivel de seguridad alto**	
10	Conocimiento de algún programa para evaluar el nivel de seguridad con que se maneja la información digital.	2%	**98%**	La evaluación de la seguridad del manejo de información es de vital importancia para el buen desempeño en el manejo de la información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.		**Bajo**
11	Evaluación de la seguridad con que se maneja la información almacenada digitalmente	33%	**64%**			**Bajo**
12	Asignación periódica del tiempo laboral para capacitaciones sobre seguridad informática	23%	**75%**	La importancia del proceso de capacitación al momento que surgen cambios informáticos en las instituciones contribuye para que las personas profesionalicen su trabajo y que sus conocimientos no queden desfasados en el uso de herramientas que les permitan manejar la información de manera más segura y eficiente.	Si el número de instituciones que posee dicha vulnerabilidad es: ◆ Mayor 30% = **Nivel de seguridad bajo** ◆ Entre 10% y 30% = **Nivel de seguridad medio** ◆ Menor al 10% = **Nivel de seguridad alto**	**Bajo**
13	Capacitaciones cuándo se realizan actualizaciones en el sistema informático	35%	**61%**			**Bajo**

14	Políticas de seguridad informática formales, escritas documentadas e informadas a todo el personal en la institución.	10%	**90%**	Las políticas informáticas son importantes para las instituciones ya que permiten concientizar acerca de la sensibilidad de la información, disminuir las amenazas a la seguridad de la información, evitar el comportamiento inescrupuloso y uso indiscriminado de los equipos que registran y resguardan la información entre otros.		**Bajo**
Si = Vulnerabilidad				**No = Fortaleza**		
				Impacto		
15	Uso de versión gratuita de antivirus	**38%**	62%	Existen programas de antivirus que son gratuitos para uso personal o para uso no comercial. En la mayoría de los casos estos antivirus gratuitos son versiones menos confiables que las versiones comerciales.(InformáticaHoy)	Si el número de instituciones que posee dicha vulnerabilidad es: ◆ Mayor 35% = **Nivel de seguridad bajo** ◆ Entre 10% y 35% = **Nivel de seguridad medio**	**Bajo**

16	Problemas de virus	**79%**	21%	Los virus son un problema muy frecuente que una vez se encuentre dentro del sistema puede generar muchos daños a este y a los archivos almacenados en la computadora, por lo que este problema debe combatirse por medio de la prevención, siendo prudentes al ingresar información por cualquier medio ya sea por internet o dispositivos externos.	◆ Menor al 10% = **Nivel de seguridad alto**	**Bajo**
17	Acceso a redes sociales en el equipo de trabajo	**36%**	63%	Nada puede garantizar que los archivos que estamos descargando de internet son seguros y no un señuelo para poder ingresar a nuestra computadora y hurtarnos modificarnos o dañarnos la información, por lo tanto las herramientas de descarga, o directamente el acceso a		**Bajo**
18	Acceso a páginas de descarga en el equipo de trabajo	**25%**	73%			**Medio**

				páginas de descarga con fines personales deben estar restringidas.		
19	Problemas de alteración de los datos	**10%**	90%	Todas las computadoras contienen alguna información de interés para alguien, no siempre tendrá el mismo valor, pero siempre puede existir alguien interesado en conseguirla, por eso es recomendable realiza monitoreos frecuentes para evaluar los posibles puntos débiles por los que puedan acceso a la información personas no autorizadas para evitar robo de información, modificación o daños.	Estos dos aspectos involucran directamente la información por lo tanto tienen el mayor grado de importantica considerado: Si el número de instituciones que posee dicha vulnerabilidad es: ◆ Mayor 9% = **Nivel de seguridad bajo** ◆ Entre 5% y 9% = **Nivel de seguridad medio** ◆ Menor al 5% = **Nivel de seguridad alto**	**Bajo**
20	Problemas de robo de información	**2%**	98%			**Alto**

Fuente: Elaboración propia[2]

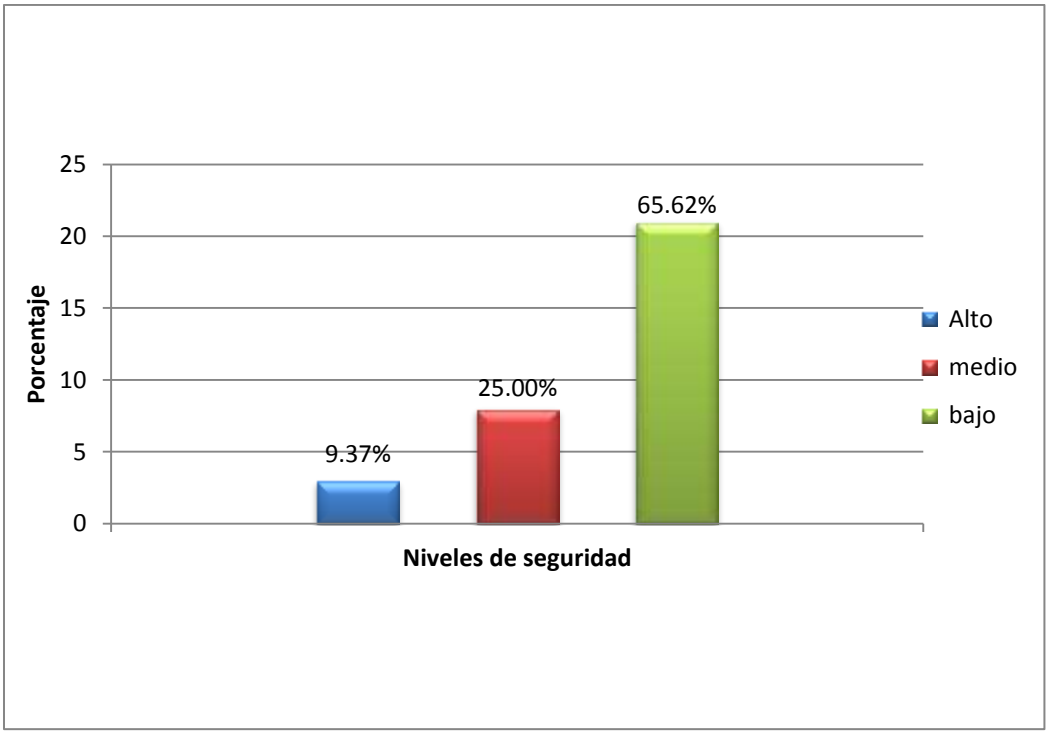
[2] Ver anexo Nº 6, pág. 260

Tabla 69: Resultados generales de los niveles de seguridad

Nivel de seguridad por criterio	Frecuencia total
Nivel de seguridad alto	3
Nivel de seguridad medio	8
Nivel de seguridad bajo	21
Total de criterios	**32**

Fuente: Elaboración propia

Gráfica 42: Nivel de seguridad en las bases de datos y redes informáticas



Fuente: Elaboración propia

4.4.2. Medidas de seguridad física para minimizar la vulnerabilidad.

Tabla 70: Medidas de seguridad para las diferentes vulnerabilidades físicas identificadas

Tipo de vulnerabilidad	Vulnerabilidades identificadas	Medidas preventivas
Vulnerabilidades de infraestructura	Ventilación inapropiada	◆ Instalar ventiladores en los lugares donde se encuentra el equipo informático que resguarda la información. ◆ Si se cuenta con computadoras portátiles instalar ventiladores individuales para cada equipo alimentados mediante USB. ◆ Cubrir con cortinas de colores claros la infiltración de los rayos solares ya que estas reflejan los rayos solares y absorben menos calor que los colores obscuros. ◆ Si el equipo está tapado con cobertores asegurarse de destaparlo completamente antes de usarlo. ◆ Evitar colocar el equipo que almacena la información sobre superficies que no disipen el calor.

	No se utilizan alarmas de seguridad	◆ Se recomienda instalar un sistema de alarmas que le permita alertar de situaciones con anomalías, para ello debe considerar los diferentes tipos de alarmas para la necesidad que se desea suplir, para elegir entre estas la que se adapte mejor a sus necesidades y presupuesto. Entre algunas de las alarmas con mayor prioridad para alertar ante las situaciones de riesgo más comunes; se recomiendan las alarmas de ingreso y las alarmas contra incendios.
	Mala ubicación del equipo que almacena la información	◆ Asignar muebles adecuados al espacio utilizado por los equipos informáticos. ◆ Reubicar en repisas o bodega el equipo informático y documentación que no se utiliza frecuentemente.
	Cortocircuitos	◆ Proteger los servidores y equipo de almacenamiento de información con un regulador de voltaje. ◆ Desconectar las conexiones eléctricas durante una tormenta eléctrica. ◆ Verificar periódicamente que los cables de suministro eléctrico no estén desprotegidos.

	Chispazos eléctricos	◆ La conexión eléctrica debe de estar debidamente polarizada. ◆ No usar extensiones o regletas para la conexión del equipo de almacenamiento. ◆ No conectar más de un equipo en un mismo tomacorriente. ◆ Solicitar la inspección de un técnico electricista para que verifique las causas de las fallas y pueda dar una solución profesional.
	Cableado de red desordenado	◆ Afianzar los cables a la pared o colocarlos dentro de canaletas. ◆ Desconectar y cambiar periódicamente cables dañados. ◆ Proveer conexiones futuras para evitar la adición de cables.
	Mal estado de los tomacorrientes	◆ Solicitar electricistas autorizados para que realicen revisiones periódicamente en las instalaciones eléctricas para verificar que estas estén en buen estado.
	Infiltración de agua	◆ Programar revisiones periódicas en techos y drenajes para verificar que no haya infiltración de agua cerca del equipo (priorizar esto en temporada de lluvias).

		◆ Verificar periódicamente que los drenajes de agua de los techos de las instalaciones que resguardan el equipo estén libres de obstrucciones. ◆ En épocas de invierno, cubrir con protectores el equipo que resguarda la información cuando este se encuentre apagado, para protegerlo de la humedad en el aire.
	Ausencia de medidas de acceso a las instalaciones del equipo que almacena la información	◆ El equipo informático que almacena la información no debe estar ubicado en las áreas de alto tráfico de personas o con un alto número de invitados. ◆ Establecer un medio de control de entrada y salida de visitas a las instalaciones donde se encuentra ubicado el equipo de almacenamiento de la información. ◆ Asignar a una o más personas la responsabilidad del control del personal que accederá a las instalaciones.
Vulnerabilidades del hardware	Sobrecalentamiento del equipo	◆ Mantener una ventilación apropiada en el ambiente del equipo ya sea con aire acondicionado o ventiladores. ◆ Ubicar el equipo lejos de la luz solar. ◆ Apagar el equipo cuando no esté en uso. ◆ Evitar cubrir las entradas de ventilación de

		los equipos. ◆ Realizar mantenimiento preventivo a las computadoras.
	Descuido del equipo	◆ Motivar al personal a reportar todos los accidentes ocurridos, los incidentes que se logren evitar, actos y condiciones que brindan poca seguridad. ◆ Instruir al personal a mantener libre de polvo las partes externas del equipo.
	Lentitud	◆ Eliminar archivos y programas no utilizados como los almacenados en la papelera de reciclaje, los archivos temporales del sistema y las cookies. ◆ Desfragmentar periódicamente el disco duro. ◆ No abrir varios programas y documentos simultáneamente. ◆ No permitir el almacenamiento de archivos personales en los equipos.
	Daños en el equipo	◆ Cuando se efectúen reparaciones al equipo, por parte de técnicos externos, deberá extraerse los archivos almacenados en el disco duro.

Vulnerabilidades de los medios o dispositivos de almacenamiento de la información	Caducidad de los medios de almacenamiento	◆ Establecer un periodo no mayor de seis meses para la revisión de los medios de almacenamiento para evitar que estos queden obsoletos.
	Uso incorrecto de los medios de almacenamiento	◆ Establecer quiénes serán las personas que tendrán acceso a los medios de respaldo de la información. ◆ Evitar el almacenamiento de información institucional en dispositivos tales como USB, debido a que con facilidad se pueden extraviar o ser hurtadas.
	Lugares inapropiados para el almacenamiento de copias de seguridad	◆ Contar con un lugar específico para el resguardo de los medios de almacenamiento que cuente con mecanismos de seguridad. ◆ Almacenar respaldos en diferentes lugares como prevención de pérdidas ante desastres naturales tales como incendios, terremotos o inundaciones.
	Consumo de alimentos cerca del equipo que almacena la información.	◆ Concientizar al personal de los riesgos a los que se exponen al consumir alimentos cerca del equipo informático que resguarda la información. ◆ Colocar letreros que señalen instrucciones para el cuido del equipo que almacena la información.

Vulnerabilidades por errores humanos	Robo	◆ Acondicionar las instalaciones de tal manera que puedan resguardar el equipo informático. ◆ No permitir el uso y acceso al equipo por usuarios no autorizados.
	Malas prácticas de los usuarios	◆ No anotar las contraseñas en agendas o notas a las que otras personas tengan acceso. ◆ No almacenar archivos de información laboral junto con archivos personales. ◆ No compartir dispositivos de almacenamiento que contengan archivos institucionales.

Fuente: Elaboración propia

4.4.3. Medidas preventivas y correctivas de seguridad lógica

Tabla 71: Medidas preventivas y correctivas para las diferentes vulnerabilidades lógicas identificadas

Tipo de vulnerabilidad	Vulnerabilidades identificadas	Medidas preventivas
Vulnerabilidades de acceso a la información	Ausencia de contraseña	◆ Implementar medidas que garanticen el uso de contraseñas en archivos que almacenen información importante.
	Contraseñas estáticas	◆ Cambiar la contraseña en lapsos no mayores de 90 días. ◆ Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al

		sistema. ◆ Las contraseñas deben ser del tipo "password fuerte" (no menor a 8 caracteres, no sean nombres, fechas de nacimiento, que combinen letra mayúsculas, minúsculas y números).
	Contraseñas compartidas	◆ Control de acceso al sistema con contraseñas individuales para cada usuario. ◆ Restricción de sesiones simultáneas. ◆ Crear bitácoras para enlistar los procesos realizados por los usuarios que hacen uso del sistema informático.
	Hurto de contraseñas	◆ Establecer contraseñas difíciles de descifrar tomando en cuenta lo siguiente: Utilizar números y letras, agregar letras mayúsculas intercaladas y su longitud no menor a 8 caracteres. ◆ Establecer cambio periódico obligatorio de la contraseña. ◆ Definir un límite de intentos fallidos para ingresar la contraseña. ◆ No habilitar opciones de recordar contraseña en el sistema. ◆ No compartir contraseñas por internet.

	Accesos no deseados	◆ Habilitar el firewall de Windows para impedir el ingreso de intrusos a la computadora vía internet. ◆ Instalar antispyware que neutralice la acción de software apropiadores de datos.
Vulnerabilidades del uso de la información	Sobrecarga de información en el equipo informático	◆ Borrar archivos que no son necesarios para realizar las actividades laborales. ◆ Almacenar en medios externos los archivos menos utilizados. ◆ Desinstalar programas que no se utilizan, para liberar espacio. ◆ Evitar el almacenamiento de archivos personales en el equipo informático perteneciente a la institución.
	Ausencia de políticas de seguridad	◆ Recopilar material de apoyo que guie en la creación de políticas. ◆ Redactar políticas de seguridad. ◆ Hacer un proceso de revisión de las políticas redactadas. ◆ Aprobar las políticas redactadas y revisadas.
	Alteración de los datos	◆ Lleve una bitácora de actividades de los usuarios.

		◆ Establezca controles para minimizar los riesgos de alteración de la información, entre estos podemos mencionar: restricciones de usuarios, monitoreo constante, entre otros. ◆ Establezca validación para ingreso de información.
	Infecciones de virus.	◆ Cerciorarse de que el antivirus este siempre actualizado. ◆ Asegurarse de que el antivirus permanezca activo. ◆ Analice siempre los archivos comprimidos. ◆ Bloquee el acceso a páginas de dudosa procedencia. ◆ Evite realizar descargas de lugares no seguros. ◆ Analice memorias USB antes de abrir su contenido. ◆ Desactive las ejecuciones automáticas de dispositivos de almacenamiento. ◆ Evite el uso de software pirata. ◆ Programe escaneos del sistema desde el

		arranque. ◆ Restaure el sistema operativo a un punto donde se encontraba estable y libre de virus. ◆ Abra memorias USB con programas tales como: Winrrar y Nero, que eviten la ejecución automática de ficheros maliciosos.
	Pérdida de información	◆ Asigne privilegios para eliminar y modificar solo a las personas que sean las responsables de estos procesos. ◆ Bloquee la computadora de trabajo al retirarse de ella.
	Ausencia de respaldos de la información	◆ Establezca qué datos se deben respaldar y con qué frecuencia. ◆ Asigne al personal responsable de realizar las copias.
	Intrusos informáticos	◆ Establezca Identificador de usuario y contraseña requerida para conectarse a la computadora de la red. ◆ Use programas anti-spyware, ya que ayuda a proteger su equipo contra ventanas emergentes, rendimiento lento y amenazas de seguridad provocadas por spyware y otro software no deseado. ◆ Mantenga actualizado el software anti-

		spyware.
	Robo de información	◆ Límite el acceso a la información. ◆ Encripte datos confidenciales. ◆ Use firewall ya que permite bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. ◆ Si desea eliminar archivos confidenciales no debe enviarlos a la papelera de reciclaje, se recomienda eliminarlos permanentemente utilizando la combinación de teclas Ctrl + Alt + Supr.
	Uso incorrecto del software	◆ Facilite manuales sobre el uso del software a los usuarios. ◆ Capacite al personal constantemente. ◆ Establezca reglas de uso para los diversos software utilizados.

Fuente: Elaboración propia

CAPÍTULO V. DESARROLLO.

Síntesis

Esta etapa comprende la elaboración del software incluyendo, requerimientos de desarrollo, requerimientos operativos, diseño de base de datos y el diseño de las interfaces del software.

5.1. DEFINICIÓN DE REQUERIMIENTOS

5.1.1. Requerimientos de desarrollo de software

Software

Para desarrollar el software propuesto en el proyecto, se necesitó hacer una elección adecuada de software de desarrollo, para ello se realizó una comparativa de las características de los diferentes software posibles de los cuales se seleccionaron los siguientes:

Tabla 72: Herramientas utilizadas para el desarrollo de la aplicación

Programa de elección	Motivo de elección
Sistema operativo: 	◆ Interfaz gráfica que facilita su uso. ◆ Rendimiento óptimo ante multiprocesos ◆ Compatibilidad con los programas de desarrollo y diseño del software. ◆ Mayor velocidad en el arranque y en la ejecución de procesos que Windows XP y Vista.
Sistema gestor de base de datos: 	◆ Experiencia previa de trabajo en él. ◆ Fácil de usar. ◆ De licencia libre. ◆ Mayor número de personas con conocimientos sobre MySQL para asesoría. ◆ Mayor disponibilidad de tutoriales.
Lenguaje de programación: 	◆ Conocimiento previo de uso ◆ Permite Integración con varias bibliotecas externas. ◆ Se caracteriza por ser un lenguaje muy rápido. ◆ Tiene compatibilidad con MySQL.

Plataforma para el desarrollo de la aplicación: 	◆ Conocimiento previo de uso. ◆ Se acopla mayormente a las necesidades de nuestro sistema. ◆ Licencia libre.
Plataforma para el diseño de la aplicación: 	◆ Tiene similitud con Corel Draw, Adobe Ilustrador y Freehand ◆ Licencia libre ◆ Calidad de diseños ◆ Fácil de utilizar ◆ Capacidad de exportación directa a PDF

Fuente: Elaboración propia

Hardware

Para el desarrollo de la aplicación debía contarse con el equipo informático que tuviera las características básicas de hardware, que soportaran los programas necesarios para el desarrollo. En la tabla siguiente mostramos los requerimientos mínimos de hardware que fueron necesarios para el desarrollo de la aplicación de forma óptima.

Tabla 73: Equipo informático utilizado para el desarrollo de la aplicación

Dispositivo	Descripción
Pantalla	Resolución de 1024x768
Microprocesador	Pentium dual core 2.0 GHz
RAM	1 GB o superior
Disco duro	120 GB o superior
Impresora	Marca: Canon Pixma Modelo: MP280

Fuente: Elaboración propia

Recurso humano

El recurso humano encargado del desarrollo de la aplicación debía contar con los conocimientos siguientes:

- Análisis de sistemas
- Diseño y desarrollo de programas
- Creación de base de datos
- Pruebas e implementación

5.1.2. Requerimientos operativos

Para que el software opere de forma correcta es necesario que se cumplan ciertos requisitos los cuales se describen continuación:

Software

Tabla 74: Software requerido para el funcionamiento de la aplicación

Categoría	Características
Sistema operativo	Windows XP ,7,8
Gestor de bases de datos	MySQL
Reproductor multimedia	Adobe Flash Player 9
Visor de documentos PDF	Adobe Reader

Fuente: Elaboración propia

Hardware

Tabla 75: Hardware necesario para el funcionamiento óptimo de la aplicación

Dispositivo	Descripción
Microprocesador	Pentium 4 o superior
RAM	512 MB o superior
Disco duro	60 GB o superior

Fuente: Elaboración propia

Recurso humano

Para que el software sea utilizado adecuadamente es importante que los usuarios que hagan uso de él tengan conocimientos básicos en:

- Paquetes de ofimática.

Solo será necesario brindar a los usuarios un manual que les guie en el uso del software desarrollado.

Seguridad

El software se encargará de la evaluación de la seguridad de las bases de datos y redes informáticas con las que trabajan las instituciones por lo tanto la manipulación y el resguardo de los resultados de estas evaluaciones deben tener un control estricto de acceso. Por lo tanto los niveles de seguridad estarán determinados por el tipo de usuario que accederá a la aplicación.

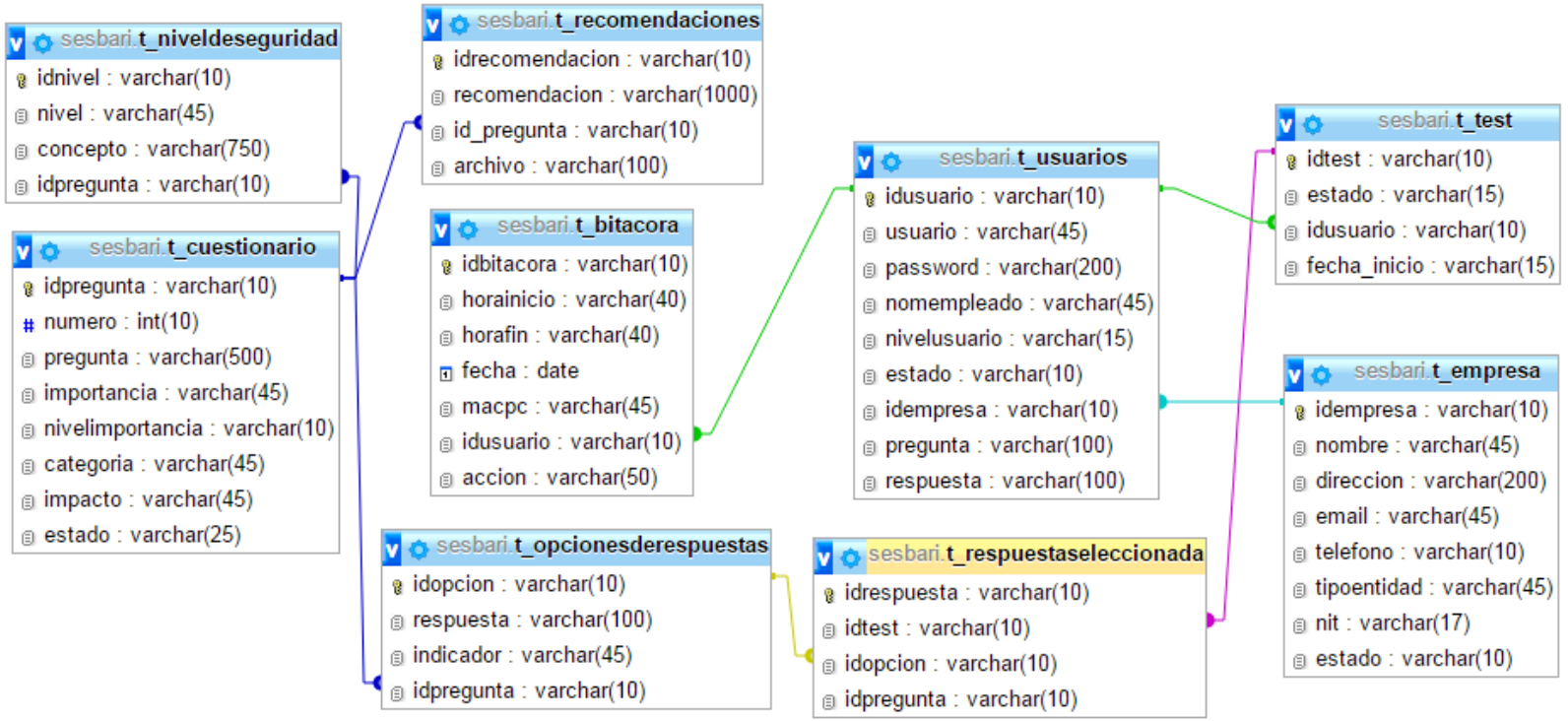
Los usuarios estarán autorizados para realizar diversas actividades dependiendo del nivel de acceso que tengan ya sea como administrador o usuario final, tendrán sus respectivas contraseñas para interactuar con la aplicación y hacer uso de los privilegios correspondientes en cada nivel de usuario.

Marco legal

El marco o entorno legal en el que funciona la aplicación fue definido por los lineamientos internos establecidos por las instituciones que harán uso de la aplicación: Los permisos otorgados a los usuarios de la aplicación, las evaluaciones realizadas con la aplicación y la implementación de las medidas correctivas proporcionadas por esta, dependen exclusivamente de la institución que haga uso de la aplicación.

5.2. DISEÑO DE BASE DE DATOS

Figura 2: Base de datos



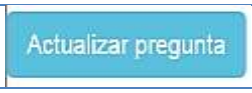
Fuente: Elaboración propia

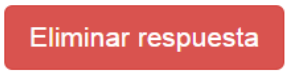
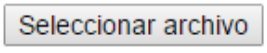
5.3. DISEÑO DEL SOFTWARE

5.3.1. Estándares de botones

A continuación se muestra la descripción del estándar de botones utilizados para realizar las diferentes operaciones en las pantallas del software, por lo que cada uno tiene funciones específicas asignadas:

Tabla 76: Estándares de botones

Nombre	Icono	Descripción
Inicio		Se utiliza para regresar al menú principal.
Conocer más sobre el software		Muestra información sobre el software
Terminar cuestionario		Permite guardar las respuestas correspondientes a cada pregunta.
Volver al submenu		Permite regresar al submenú de cuestionario por áreas.
Guardar pregunta		Este botón permite guardar una nueva pregunta que será introducida por completo.
Agregar nueva pregunta		Permite agregar una nueva pregunta después de haber introducido una pregunta inicial sin necesidad de regresar al menú principal.
Cambiar pregunta		Permite hacer cambios a una pregunta diferente desde el formulario actualizar pregunta sin necesidad de regresar al menú principal.
Actualizar		Sirve para confirmar si se desean

pregunta		guardar los cambios que permiten actualizar una pregunta.
Agregar respuesta		Permite agregar una o varias respuestas a una pregunta.
Eliminar respuestas		Sirve para eliminar una respuesta.
Actualizar respuesta		Permite actualizar respuesta dentro del formulario ACTUALIZAR PREGUNTA.
Editar respuesta		Llama al formulario de edición de respuestas.
Actualizar		Este botón llama al formulario actualizar desde una pregunta en particular.
Eliminar		Permite eliminar una pregunta directamente.
Actualizar empresa		Sirve para actualizar los datos cambiantes de una empresa.
Actualizar usuario		Permite actualizar los datos de un usuario.
Ver reporte		Permite ver un reporte.
Ver PDF		Permite enviar un reporte a PDF.
Confirmar		Sirve para confirmar si el usuario está seguro de realizar la acción de eliminar.
Seleccionar archivo		Permite seleccionar archivos PDF para poder subirlos al software.

Fuente: Elaboración propia

5.4. DISEÑO DE INTERFACES

A continuación se describen las interfaces del software denominado “Software para la evaluación de la seguridad de las bases de datos y redes informáticas” que se identifica con el nemónico SESBARI, el cual ha sido diseñado para que las ONG´s, entidades públicas y empresas privadas puedan evaluar el nivel de seguridad de sus bases de datos y redes informáticas.

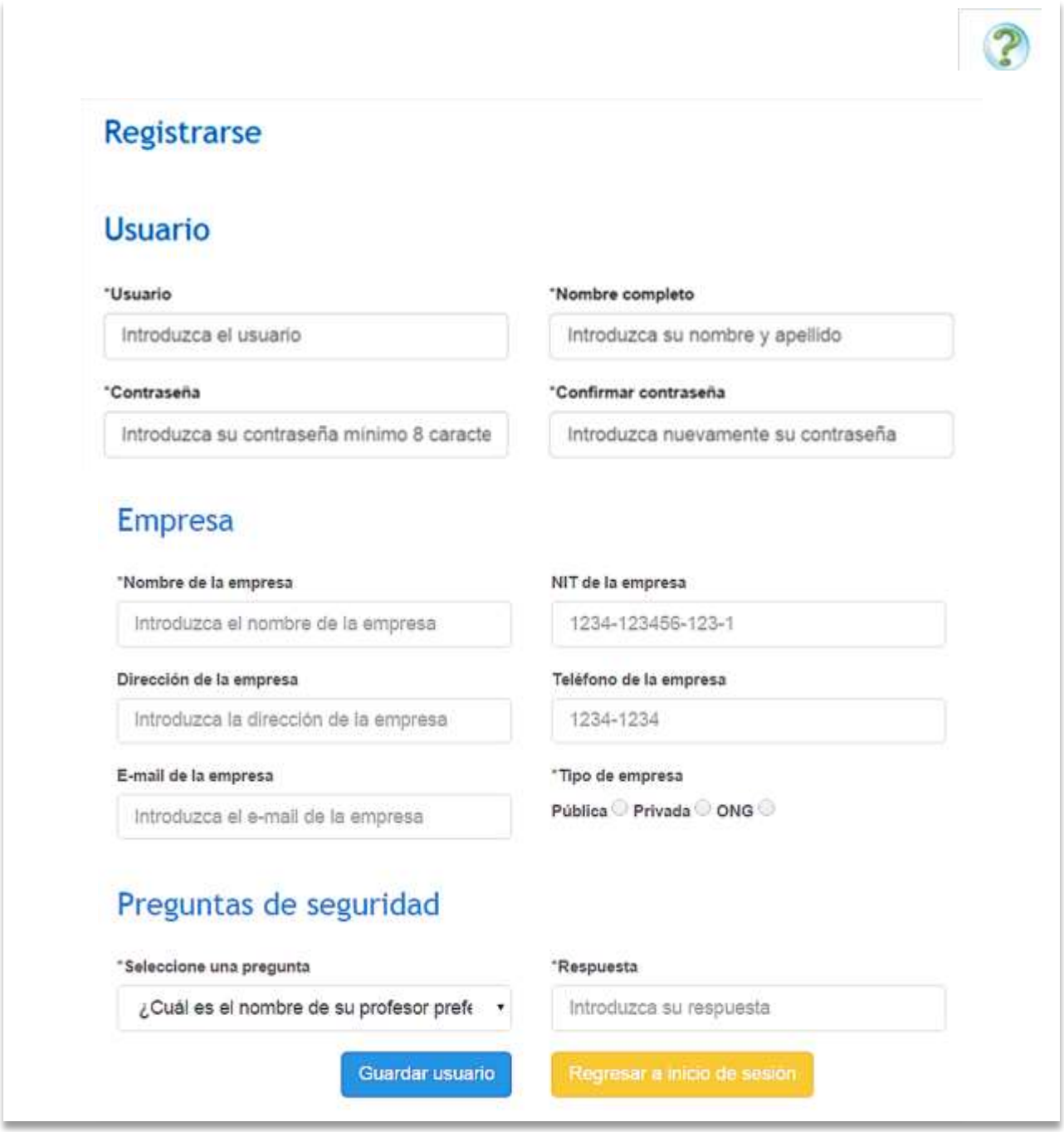
PANTALLA DE ACCESO AL SISTEMA

INICIO DE SESIÓN

El inicio de sesión permite al usuario ingresar al sistema por medio de un usuario y contraseña previamente registrada, en caso de no estar registrado brinda el acceso para registrarse por primera vez por medio del enlace registrarse, solicitando a continuación los datos del usuario y los datos de la empresa a la cual pertenece dicho usuario**.**

REGISTRAR USUARIO Y EMPRESA

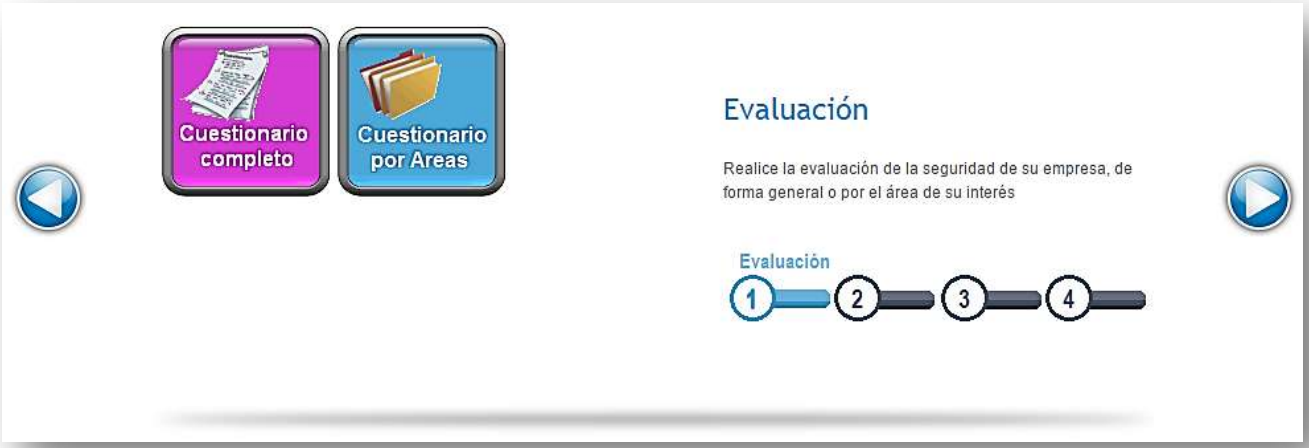
Registrar usuario y empresa es una pantalla de captura de datos, que se utiliza únicamente cuando un usuario ingresa por primera vez, garantizando que el usuario guardará en el software un registro de usuario y los datos de su empresa tales como: Nombre, NIT, dirección, email, teléfono y tipo de empresa.



MENÚ PRINCIPAL

El menú principal del software es el que da acceso a todas las opciones disponibles en él y está dividido en cuatro áreas principales, las cuales son: Evaluación, consultas y reportes, actualización y mantenimiento, estas áreas se detallan a continuación.

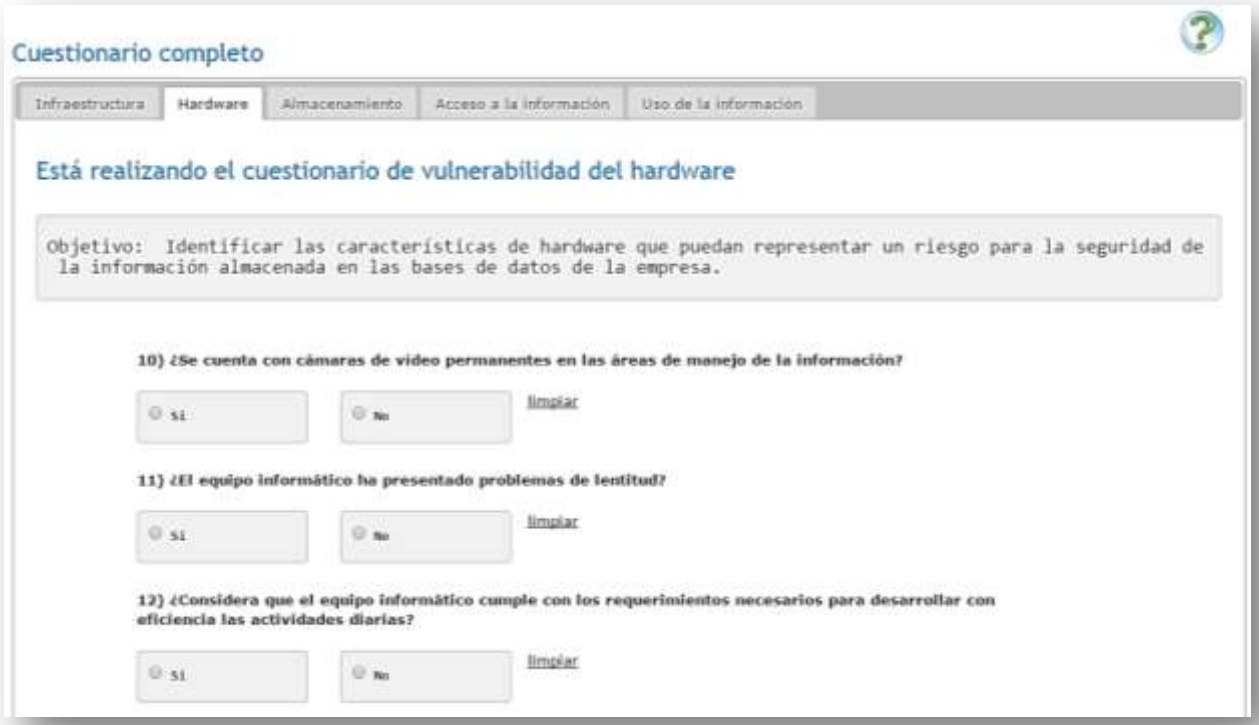
EVALUACIÓN



En el área de menú evaluación se encuentran contempladas las opciones correspondientes a la evaluación de la seguridad de las entidades que hagan uso del software, conteniendo los siguientes módulos de evaluación:

Cuestionario completo: Muestra el cuestionario de seguridad de las bases de datos y redes informáticas para hacer una evaluación completa de todas las áreas de seguridad que se evalúan en el software.

Cuestionario completo

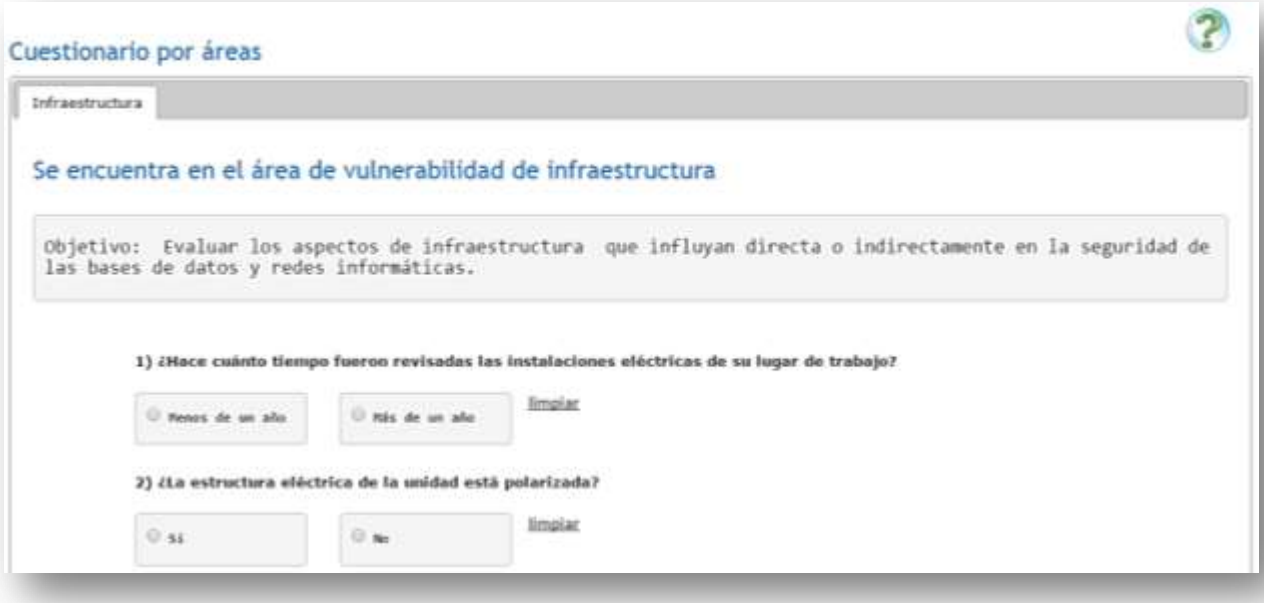


Esta pantalla muestra las cinco áreas que se consideraron en la seguridad física y seguridad lógica, para el área física se encuentran: vulnerabilidades de infraestructura, vulnerabilidades del hardware, vulnerabilidades de los medios o dispositivos de almacenamiento de la información, y para el área lógica: vulnerabilidades de acceso a la información y vulnerabilidades de uso de la información.

Dichas áreas contienen una serie de preguntas que el usuario deberá responder según sea el caso, seleccionando la opción de respuesta por medio de un radio buttom, el cual podrá ser deseleccionado con la opción “limpiar”, el objetivo de esta pantalla es evaluar el nivel de seguridad que tiene la institución u organización que está siendo evaluada, por medio del cuestionario que permite saber las debilidades y fortalezas que posee la empresa.

Cuestionario por áreas: Permite realizar la evaluación por áreas específicas por medio de un submenú el cual contiene cada una de las sub-áreas que podrán ser evaluadas por separado según lo desee el usuario.

Cuestionario por áreas



Las sub-áreas comprendidas en este sub menú son:

Vulnerabilidad de infraestructura: En esta pantalla se evalúan las vulnerabilidades relacionadas con la infraestructura de la institución en la cual el usuario deberá responder a una serie de preguntas seleccionando una opción de respuesta de las que se presentan, al final de la evaluación el usuario podrá ingresar las observaciones pertinentes y guardar dicha evaluación.

Vulnerabilidad del hardware: En esta pantalla se evalúa las vulnerabilidades relacionadas con el hardware con que cuenta la institución para identificar si las condiciones de este representan riesgo para la seguridad de la información, por lo que el usuario deberá responder a las preguntas que se presentan en dicha pantalla y posteriormente guardar la evaluación realizada con sus respectivas observaciones si las hubieran.

Vulnerabilidad de los medios o dispositivos de almacenamiento de la información: Es una pantalla en la cual el usuario puede realizar una evaluación referente a las vulnerabilidades que puedan tener los medios de almacenamiento que la institución utiliza para respaldar o almacenar la información con la que trabaja.

Vulnerabilidad de acceso a la información: El usuario puede evaluar el nivel de seguridad en lo referente a las formas de acceso y los mecanismos de seguridad implementados al momento de acceder a la información.

Vulnerabilidad de uso de la información: Se evalúan las practicas realizadas por los usuarios de la información, y los procesos utilizados para su manejo para verificar que tan vulnerable o protegida esta la información ante las amenazas que se presenten.

CONSULTAS Y REPORTES

El menú de consultas y reportes da acceso a tres áreas que ofrecen información al usuario, siendo estas áreas: la bitácora de procesos, el nivel de seguridad que se obtuvo de la

evaluación por medio del cuestionario y las recomendaciones necesarias para superar las vulnerabilidades de seguridad de la información detectadas por el software. Cada una de estas consultas dará acceso a su respectivo reporte en PDF que podrá imprimirse o guardarse como un archivo interno o en medios de almacenamiento externos.

Bitácora


Reporte de bitácora

Acción	Fecha	Hora de incio	Hora de finalización	IP	Usuario
Almacenamiento de cuestionario	2014-12-01	03:47:33	03:47:33	190.87.24.26	super user
Almacenamiento de cuestionario	2014-12-01	03:52:40	03:52:40	190.87.24.26	super user
Almacenamiento de cuestionario	2014-12-01	03:52:23	03:52:23	190.87.24.26	super user
Almacenamiento de cuestionario	2014-12-01	03:53:11	03:53:11	190.87.24.26	super user
Almacenamiento de cuestionario	2014-12-01	03:52:55	03:52:55	190.87.24.26	super user
Acción	Fecha	Hora de incio	Hora de finalización	IP	Usuario

Muestra la bitácora del sistema donde se podrán consultar los datos de los usuarios que han accedido al sistema y de las tareas que han realizado en él.

El usuario final únicamente visualiza las actividades realizadas por sí mismo en las diferentes fechas, el administrador podrá consultar sus actividades y la de los usuarios de su empresa u organización.

Nivel de seguridad

Consulta del nivel de seguridad general (gráfica): Esta consulta muestra cual es el nivel de seguridad de la entidad que se está evaluando, con relación a las dos áreas generales de la evaluación siendo estas: seguridad física y lógica, mostrando la información de forma tabulada y gráfica. (Ver anexo Nº 8 pág. 268).

Consulta del nivel seguridad lógica (grafica): Esta consulta proporciona el nivel de seguridad identificado en cada una de las sub áreas comprendidas en la seguridad lógica, siendo estas: el área de vulnerabilidades del acceso a la información y de vulnerabilidades del uso de la información, además muestra el resultado general de la evaluación del área lógica.

Consulta del nivel de seguridad física (grafica): Esta consulta proporciona el nivel de seguridad identificado en cada una de las sub áreas comprendidas en la seguridad física, siendo estas: el área de vulnerabilidades de infraestructura, de vulnerabilidades del hardware, vulnerabilidades de los medios o dispositivos de almacenamiento de la información, además muestra el resultado general de la evaluación del área física.

Consulta del nivel de seguridad lógica por áreas (grafica): Se muestran las consultas individuales correspondientes a cada una de las áreas consideradas en la seguridad lógica, los cuales se detallan a continuación: Consulta de vulnerabilidades de acceso a la información y consulta de vulnerabilidades del uso de la información.

Consulta del nivel de seguridad física por áreas (grafica): Se muestran las consultas individuales correspondientes a cada una de las áreas consideradas en la seguridad física, los cuales se detallan a continuación: Consulta de vulnerabilidades de infraestructura, reporte de vulnerabilidades del hardware y consulta de vulnerabilidades de los medios o dispositivos de almacenamiento de la información.

Recomendaciones

Consulta de recomendaciones generales: Muestra una consulta con las recomendaciones para mejorar la seguridad de la información en todas las áreas de evaluación del software en las que se han identificado vulnerabilidades en la seguridad de la información de la empresa evaluada. (Ver anexo Nº 8, pág. 268).

Consulta de recomendaciones del área lógica: En esta opción se proporciona la consulta de recomendaciones correspondiente a las áreas comprendidas en la seguridad lógica en las que se detectaron vulnerabilidades por medio del software.

Consulta de recomendaciones del área física: Se muestran las recomendaciones para superar las vulnerabilidades de seguridad física identificadas por medio del software,

clasificadas en cada una de las sub áreas de la seguridad física y presentadas como una única consulta.

Consultas de recomendaciones para seguridad lógica por área: Por medio de esta opción se muestra el conjunto de consultas de recomendaciones individuales para cada una de las sub áreas de la seguridad física.

Consultas de recomendaciones para seguridad física por áreas: Por medio de esta opción se muestra el conjunto de consultas de recomendaciones individuales para cada una de las sub áreas de la seguridad lógica.

ACTUALIZACIÓN

Esta área del menú permite actualizar los datos del usuario del sistema como los datos de la empresa a la que pertenece el usuario.

Actualizar usuario

Una vez iniciada sesión el usuario podrá actualizar su nombre de usuario o su contraseña por medio de la siguiente pantalla.

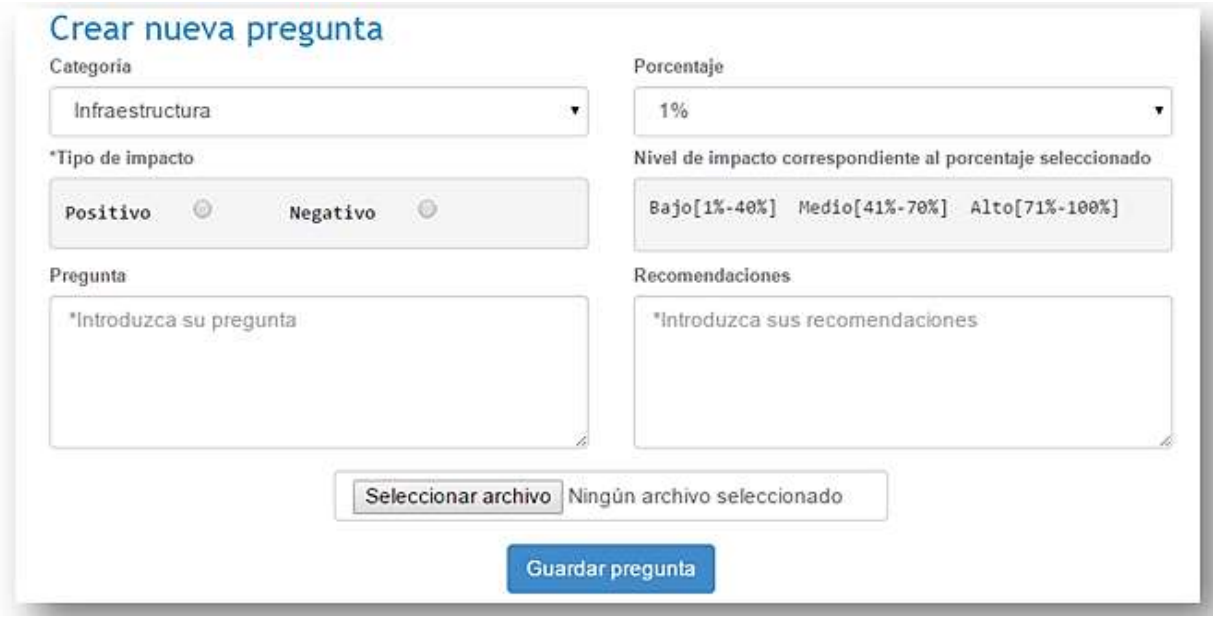
Actualizar empresa

En esta pantalla se actualizan los datos de las empresas registradas en el software, el usuario podrá modificar únicamente los datos de la empresa a la cual pertenece para ello únicamente deberá ingresar a esta pantalla que mostrará los datos de la empresa automáticamente y deberá proceder a actualizar los datos correspondientes, los cuales pueden ser: Dirección, e-mail, tipo de empresa y teléfono.

MANTENIMIENTO

En el área de menú mantenimiento se encuentran las opciones que permiten darle mantenimiento a las preguntas de evaluación, como también agregar nuevas preguntas al software, estas opciones serán visualizadas únicamente por los usuarios con privilegios de administrador, las vistas a las que dan acceso estas opciones del menú se describen a continuación:

Nueva pregunta



La pantalla de crear nueva pregunta es la pantalla que permite al usuario administrador interactuar con el software y mantenerlo actualizado con aquellos aspectos de seguridad que no se hayan considerado originalmente.

El usuario primeramente deberá de seleccionar en cuál de las cinco categorías se ubica mejor su nueva pregunta, el software internamente le asignará un número correlativo a la pregunta, el usuario deberá de introducir aspectos importantes tales como: el impacto que esta pregunta representa para su empresa ya sea positivo o negativo, el enunciado de la pregunta, y el porcentaje de importancia que esta pregunta representa para su institución el cual podrá estar en un rango respectivo del 1% al 100%, además deberá ingresar las recomendaciones correspondientes para la pregunta que se está almacenando, si la recomendación requiere de un plantilla modelo esta se podrá anexar a las recomendaciones con el botón “Seleccionar archivo”. Está permitido almacenar en el software tantas preguntas como sea necesario.

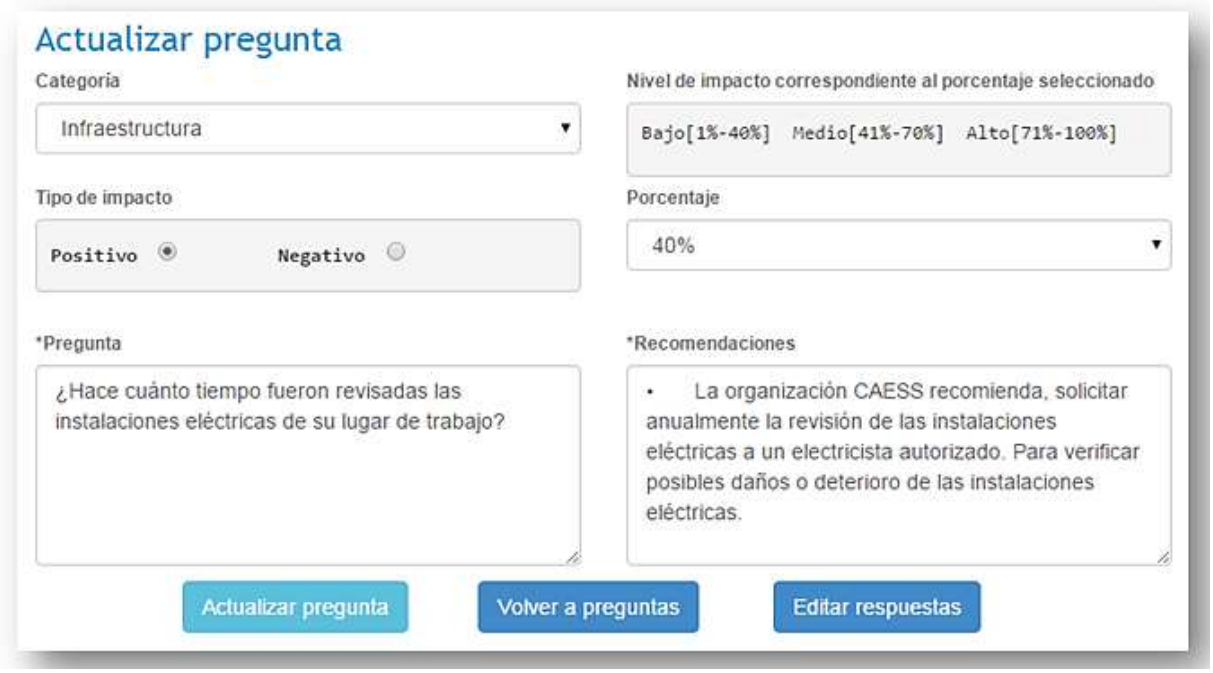
Al guardar la pregunta con todos sus elementos se mostrara la siguiente pantalla para finalizar con el proceso de agregar nueva pregunta:

Actualizar pregunta

Esta pantalla permite al usuario administrador eliminar las preguntas que hayan quedado obsoletas por los cambios de las tecnologías y actualizar las preguntas que considere

necesario, cambiando la redacción o eliminando y agregando elementos de texto a la pregunta en caso que ya hayan quedado desfasadas o si desea agregarle algo más a las recomendaciones de estas, para ello el usuario deberá elegir la categoría y seleccionar ya sea la opción de actualizar o eliminar para cada pregunta.

Al seleccionar la opción actualizar el sistema le mostrará los datos de la pregunta seleccionada para proceder a modificarla permitiéndole editar el criterio para dicha pregunta, además mostrará el impacto que esta tenga ya sea negativo o positivo el cual podrá modificarse dependiendo de la actualización de la pregunta que el usuario realice, de igual forma el porcentaje de importancia que presenta podrá actualizarse considerándose si es nivel bajo, medio o alto y finalmente podrá editarse la recomendación correspondiente a la pregunta.



La vista a la que da acceso el botón editar respuestas de la imagen anterior permite al usuario administrador eliminar o modificar cada una de las respuesta que fueron asignadas a la pregunta que se está modificando.

5.5. DESCRIPCIÓN DE LA METODOLOGÍA

La programación orientada a objetos es una metodología de programación avanzada y bastante extendida, en la que los sistemas se modelan creando clases, que son un conjunto de datos y funcionalidades. Las clases son definiciones, a partir de las que se crean objetos. Los objetos son ejemplares de una clase determinada y como tal, disponen de los datos y funcionalidades definidos en la clase.

Durante años, los programadores se han dedicado a construir aplicaciones muy parecidas que resolvían una y otra vez los mismos problemas. Para conseguir que los esfuerzos de los programadores puedan ser utilizados por otras personas se creó la POO. Que es una serie de normas de realizar las cosas de manera que otras personas puedan utilizarlas y adelantar su trabajo, de manera que consigamos que el código se pueda reutilizar, esta es una razón por la que un mayor número de lenguajes adoptan la programación orientada a objetos, prueba de ello es la nueva versión de PHP (5), que implanta la programación de objetos como metodología de desarrollo.

Para el desarrollo del Sistema Informático SESBARI la metodología utilizada fue la de programación orientada a objetos; ya que ofrece las siguientes ventajas.

1. Reutilización de código.
2. Facilidad en la creación de diseños visuales.
3. Se agiliza el desarrollo de software.
4. La programación es más fácil de entender.
5. Al dividir el software en partes más pequeñas podemos probarlo de manera independiente y aislar mucho más fácilmente los posibles errores que puedan surgir.

(Hernández, (s.f.), pp. 4-8)

5.6. MANUAL DE USUARIO

Para mayor información consulte CD ***SESBARI/Manuales/manual de usuario***

BIBLIOGRAFÍA

Libros

Meléndez M. R. (2012) Como preparar el anteproyecto de investigación y la tesis de graduación. San Salvador: Ediciones Myssa.

Internet

Marroquín, W., Argueta Quan, R., Quintanilla Juárez, N. A., Ibarra, A. R., Duque de Rodríguez, A. L., Alegría Coto, J.,… & Trujillo Martínez C. U. (2012) Indicadores de Ciencia y Tecnología 2011. Recuperado de http://www.conacyt.gob.sv/index.php?option=com_phocadownload&view=category&id=2:publicaciones&Itemid=115

Belloso Urbina, R. A., Mancia Rivera, M. N., Morán Bautista, O. J., Olmedo Portillo, G. B. (2008) Estudio y análisis sobre la informática forense en El Salvador. (Tesis de maestría inédita). Universidad de El Salvador. Recuperado de http://ri.ues.edu.sv/3190/

Melara, G., Clercx, L., Vásquez, A. P., Goitia, R., de León, M., Martínez, F.(2004) Plan de Desarrollo del Departamento de San Vicente. Recuperado de http://www.sanvicenteproductivo.org/po/PDL%20TOMO%20II.pdf

Gámez Acuña, M. V. (2002). Una Valoración de Amenazas y Propuesta de Seguridad de Depósitos de Datos (Tesis de maestria inédita) Instituto Tecnológico de Costa Rica. Costa Rica. Recuperado de http://repositoriotec.tec.ac.cr/handle/2238/213

Campos Paré, R., Casillas Santillán, L. A., Costal Costa, D., Ginestá, M. G (2005).Bases de datos. (Tesis de maestría inédita).Universidad Oberta de Cataluña. Cataluña. Recuperado de http://www.uoc.edu/masters/oficiales/img/913.pdf

Sánchez, R. B. (s.f.). Seguridad en redes. (Tesis de ingeniería inédita).Universidad Autónoma del Estado de Hidalgo. Hidalgo. Recuperado de http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf

Monge Ivars, J., Ángel, J. P. (s.f.). Estadística no paramétrica: Prueba Chi-Cuadrado X. Recuperado de http://www.uoc.edu/in3/emath/docs/Chi_cuadrado.pdf

Hernández, R. R. (s.f.). Introducción al paradigma de la Programación Orientada a Objetos (POO). Recuperado de http://www.itnuevolaredo.edu.mx/takeyas/apuntes/poo/Apuntes/01.-%20Introduccion%20a%20la%20POO.pdf

Dirección General de Estadísticas Y Censos. (DIGESTYC) (2011-2012).Documento directorio de unidades económicas. Recuperado de http://www.digestyc.gob.sv/index.php/novedades/avisos/aviso-empresa/264-directorio-de-unidades-economicas-2011-2012.html

Olaechea, H. A. (2006). Glosario básico de términos estadísticos. Recuperado de http://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib0900/Libro.pdf

MicrosoftStore. (s.f.). Ofertas destacadas. Recuperado de www.microsoftstore.com/store/msstore/en_US/pd/Project-2010-Spanish/productID.216566600

Compañía de Alumbrado Eléctrico de San Salvador. (CAESS) (s.f.). Simulador de Consumo Eléctrico Residencial. Recuperado de http:// www.aeselsalvador.com/ simulador/ Simulador2.html

Claro. (s.f.). Claro personas. Recuperado de http://www.claro.com.sv/ wps/portal/sv/ pc/personas/internet/ internet-residencial

ANEXOS

6.1. Anexo 1: Cuadro de unidades económicas y personal ocupado por municipio

Unidades económicas y personal ocupado por municipio

MUNICIPIO	TOTAL	
	UNIDADES ECONÓMICAS	Personal Ocupado
TOTAL	3,117	6,953
APASTEPEQUE	180	327
GUADALUPE	89	147
SAN CAYETANO ISTEPEQUE	28	41
SANTA CLARA	27	45
SANTO DOMINGO	68	259
SAN ESTEBAN CATARINA	71	130
SAN ILDEFONSO	64	112
SAN LORENZO	63	119
SAN SEBASTIAN	231	462
SAN VICENTE	1,846	4,362
TECOLUCA	337	779
TEPETITAN	44	65
VERAPAZ	69	105

Fuente: Directorio de unidades económicas

(Dirección General de Estadísticas y Censos, 2011-2012, p. 70)

6.2. Anexo 2: Instituciones incluidas en el estudio

Instituciones públicas

N°	Nombre	Municipio
1	Alcaldía Municipal de San Vicente	San Vicente
2	CENTA San Vicente	San Vicente
3	Instituto Nacional de los Deportes de El Salvador (INDES)	San Vicente
4	Procuraduría General de la República Unidad Auxiliar	San Vicente
5	Centro Judicial Dr. Sarbelio Navarrete	San Vicente
6	Centro Nacional de Registro (CNR)	San Vicente
7	Juzgado de Ejecución de Medidas al Menor	San Vicente
8	PNC Delegación Central	San Vicente
9	Junta de la Carrera Docente San Vicente	San Vicente
10	Procuraduría para la Defensa de los Derechos Humanos	San Vicente
11	Hospital Nacional Santa Gertrudis	San Vicente
12	Instituto Salvadoreño del Seguro Social (ISSS)	San Vicente
13	Ministerio de Agricultura y Ganadería, Dirección General de Ganadería, Regional III San Vicente	San Vicente
14	Juzgado de vigilancia Penitenciaria y de Ejecución de la Pena San Vicente	San Vicente
15	Asamblea legislativa, Oficina Departamental	San Vicente
16	Ministerio de Agricultura y Ganadería (MAG)	San Vicente

17	Junta de Protección de la Niñez y la Adolescencia (CONNA)	San Vicente
18	Juzgado de Menores	San Vicente
19	Centro de Atención Psicosocial	San Vicente
20	Fundación Ayúdame a Vivir San Vicente	San Vicente
21	Ministerio de Gobernación	San Vicente
22	Instituto Salvadoreño de Bienestar Magisterial (ISBM)	San Vicente
23	Universidad de El Salvador (UES)	San Vicente
24	Dirección Departamental de Educación de San Vicente	San Vicente
25	Correos El Salvador, San Vicente	San Vicente
26	Alcaldía Municipal de San Sebastián	San Sebastián
27	Centro Judicial de San Sebastián	San Sebastián
28	Correos El Salvador, San Sebastián	San Sebastián
29	PNC Delegación Central	San Sebastián
30	Alcaldía Municipal de Apastepeque	Apastepeque
31	Correos El Salvador, Apastepeque	Apastepeque
32	Casa de la cultura, Apastepeque	Apastepeque
33	Policía Nacional Civil (PNC)	Apastepeque
34	Juzgado de Paz	Apastepeque
35	Unidad de Salud	Apastepeque
36	Alcaldía Municipal de Tecoluca	Tecoluca

37	Juzgado de Paz, Tecoluca	Tecoluca
38	Instituto Salvadoreño de Transformación Agraria	Tecoluca
39	CENTA	Tecoluca
40	Ministerio de Medio Ambiente y Recursos Naturales	Tecoluca

Empresas privadas

Nº	Nombre	Municipio
1	Food Mark Texaco	San Vicente
2	Centro de Servicio Duramil	San Vicente
3	Cooperativa Financiera Unidad ACODJAR de R. L.	San Vicente
4	Distribuidora Agrícola Veterinaria	San Vicente
5	Clínicas Unidas	San Vicente
6	Farmacia Navarrete	San Vicente
7	Farmacia Vicentina	San Vicente
8	Farmacia la Buena	San Vicente
9	Farmacia Don Bosco	San Vicente
10	Negocio los Ángeles sucursal	San Vicente
11	Agencia de Viajes América Rosy's	San Vicente
12	Autorepuestos Vicentinos	San Vicente
13	Agro servicio Tierra Fértil	San Vicente
14	Atlantis	San Vicente
15	Almacenes Casa San Antonio	San Vicente

16	Ferretería La pulgada Sucursal	San Vicente
17	Sur Line Premium	San Vicente
18	Hospital Divino Niño	San Vicente
19	Papel y Tijera Librería y papelería "El Almacén del Maestro"	San Vicente
20	Lubricentro Charle's	San Vicente
21	Mi Casa Ferretera	San Vicente
22	Descanso	San Vicente
23	TONSA	San Vicente
24	Inversiones Casa de la Opción	San Vicente
25	FOMENTA	San Vicente
26	Supermercado Divina Providencia	San Vicente
27	Ingenio Jiboa	San Vicente
28	Alba El Camino	San Vicente
29	Gasolinera PUMA S. V.	San Vicente
30	Caritas San Vicente	San Vicente
31	Escuela de Manejo "Chirino"	San Vicente
32	Clínica Médica de Diagnostico Nuestro Señor de Esquipulas	San Vicente
33	ACAASS de R. L.	San Sebastián
34	Cooperativa Financiera Unidad ACODJAR de R. L.	San Sebastián
35	Comercial Durán S.A de C.V	Apastepeque
36	El Roble, Tecoluca	Tecoluca
37	El Roble el playón, Tecoluca	Tecoluca

Instituciones no gubernamentales (ONG'S)

Nº	Instituciones	Municipio
1	Intervida	San Vicente
2	Hábitat para la Humanidad	San Vicente
3	San Vicente Productivo	San Vicente
4	Asociación para la Organización y Educación Empresarial Femenina de El Salvador (OEF)	San Vicente
5	Aldeas Infantiles SOS San Vicente	San Vicente
6	Solidar SUIZA	Tecoluca
7	Fundación CORDES	Tecoluca

6.3. Anexo 3: Encuesta sobre la seguridad de la información.

UNIVERSIDAD DE EL SALVADOR
FACULTAD MULTIDISCIPLINARIA PARACENTRAL
DEPARTAMENTO DE INFORMÁTICA
INGENIERÍA DE SISTEMAS INFORMÁTICOS

ENCUESTA SOBRE SEGURIDAD DE LA INFORMACIÓN

DIRIGIDA A USUARIOS QUE MANEJAN INFORMACIÓN DIGITAL

Objetivo: Obtener información sobre el nivel de seguridad en las bases de datos y redes informáticas de instituciones públicas, empresas privadas y organizaciones no gubernamentales del departamento de San Vicente.

Indicación: Marque con una "**x**" la/las opción/es que considere correctas.

Datos del usuario que maneja información digital	
Cargo :	
Grado Académico:	Educación Básica ○ Educación Media ○ Educación Superior ○ Ninguno ○
Tipo de entidad:	Institución Pública ○ Empresa Privada ○ ONG's ○
Municipio al que pertenece la institución:	Apastepeque ○ San Vicente ○ San Sebastián ○ Tecoluca ○

1. ¿En su lugar de trabajo se cuenta con un departamento de informática interno?
   Si ○ No ○ No sabe ○
2. ¿En su lugar de trabajo se cuenta con los recursos económicos para la compra de equipo informático?
   Si ○ No ○ No sabe ○
3. ¿En su lugar de trabajo poseen herramientas para realizar el mantenimiento del equipo informático?
   Si ○ No ○ No sabe ○
4. ¿La asistencia técnica al equipo informático de su lugar de trabajo es proporcionada por?

Técnicos de sede central ○ Tecnicos locales ○ Tecnicos por contrato temporal ○ No recibo asistencia ○ No sabe ○

5. ¿En caso de fallos en el equipo y/o en la red en cuanto tiempo aproximadamente recibe asistencia técnica?

   Inmediatamente ○ De 1 a 5 días ○ De 6 a 15 días ○ De 16 a 30 días ○

   Más de 30 días ○ No recibo asistencia ○ No sabe ○

6. ¿En su lugar de trabajo se ha invertido presupuesto en los últimos dos años en la compra de programas informáticos actualizados?

   Si ○ No ○ No sabe ○

7. ¿En su lugar de trabajo le evalúan la seguridad con que maneja la información almacenada digitalmente?

   Si ○ No ○ No sabe ○

8. ¿Conoce algún programa para evaluar el nivel de seguridad con que se maneja la información digital de la institución donde labora?

   Si ○ Nombre del programa: _____ No ○

9. ¿Cuentan localmente con un programa que les permita evaluar la seguridad de las bases de datos y redes informáticas? (No se consideran los antivirus).

   Si ○ No ○ No sabe ○

10. ¿En el último año se ha invertido presupuesto en aspectos que contribuyan en la mejora de la seguridad de la información perteneciente a la institución donde labora?

    Si ○ No ○ No sabe ○

11. ¿En su lugar de trabajo se asigna periódicamente parte del tiempo laboral, a capacitaciones sobre seguridad informática?

    Si ○ No ○ No sabe ○

12. ¿Cada cuánto tiempo recibe cursos de actualización sobre seguridad informática?

    Mensual ○ Semestral ○ Anual ○ No recibe ○

13. ¿Cuál de las siguientes afirmaciones describe mejor la condición de las políticas de seguridad informática en su lugar de trabajo?

    No se tienen políticas de seguridad definidas ○ Actualmente se encuentran en desarrollo ○ No sabe ○

    Política formal, no implementada ○ Política formal, escrita documentada e informada a todo el personal ○

14. ¿Hace uso de las siguientes herramientas en su equipo de trabajo? (selección múltiple)

    Skype ○ Atube Catcher ○ Ares ○

    Emule ○ Ninguno ○ Otros:_____

15. Cuándo se realizan actualizaciones en el sistema informático ¿Se imparten las capacitaciones necesarias?

Si ○ No ○ No sabe ○

16. La información que maneja en su lugar de trabajo es de carácter:

Público ○ Privado ○ Ambos ○

17. ¿Utiliza contraseña para acceder a la información que almacena en su equipo de trabajo?

Si ○ No ○

18. ¿Cada cuánto tiempo cambia la contraseña de acceso a los datos que maneja en su lugar de trabajo?

Quincenal ○ Mensual ○ Semestral ○

Anual ○ Nunca ○ No utilizo contraseña ○

19. ¿Se ha enfrentado a alguna de las siguientes amenazas de seguridad de la información? (selección múltiple)

Alteración de los datos ○ Hurto de contraseñas ○ Intrusos informáticos ○ Robo de información ○

Virus ○ Ninguno ○ No sabe ○ Otro:_____

20. ¿Cuáles de los siguientes medios utiliza actualmente en su lugar de trabajo para almacenar las copias de seguridad? (selección múltiple)

Respaldo en discos duros ○ Respaldos en CD ○ Respaldos en USB ○

Ninguno ○ No sabe ○ Otros:_____

21. -¿Se almacena alguna copia de seguridad fuera de los locales de trabajo?

Si ○ No ○ No sabe ○

22. La versión del antivirus utilizado en su lugar de trabajo es:

Gratuita ○ Pagada ○ No sabe ○ No se cuenta con antivirus ○

23. ¿Seleccione los problemas de infraestructura que representan riesgo para los equipos que almacenan la información en su lugar de trabajo? (selección múltiple)

Mala ubicación de tomacorrientes ○ Tomacorrientes insuficientes ○ Ventilación inapropiada ○

Infiltración de agua ○ Poco espacio ○ No sabe ○ Ninguno ○ Otros:_____

24. ¿El equipo Informático en que trabaja ha presentado problemas de sobrecalentamiento?

Si ○ No ○ No sabe ○

25. ¿En su lugar de trabajo se han presentado casos de robo de equipo informático?

Si ○ No ○ No sabe ○

26. ¿Aproximadamente cuánto tiempo tiene de uso la computadora en que trabaja?

Menos de 1 año ○ De 1 a 2 años ○ De 3 a 5 años ○ Más de 5 años ○

27. ¿En su lugar de trabajo cuentan con alguno de los siguientes tipos de red? (Selección múltiple).

Red cableada ○ Red inalambrica ○ Ninguno ○ No sabe ○

28. ¿En su lugar de trabajo utiliza internet para acceder a la información que maneja?

Si ○ No ○ No sabe ○

29. ¿Cuál de las siguientes razones ha afectado el buen funcionamiento de su equipo informático? (selección múltiple)

Falta de limpieza rutinaria ○ Mala ubicación del equipo ○

Espacio reducido para la ubicación del equipo ○ Falta de aire acondicionado ○

Chispazos eléctricos en los tomacorrientes ○ Ninguno ○ Otras:_____

30. ¿El equipo informático que almacena la información se encuentra expuesto a la afluencia de personas ajenas a la institución donde labora?

Si ○ No ○

31. ¿Su equipo informático ha presentado alguno de los siguientes fallos de rendimiento? (selección múltiple)

Lentitud ○ Congelamiento de pantallas ○ Apagones ○ Ninguno ○

Otros:_____

32. ¿Qué tipo de mantenimiento se realiza en el equipo informático de su lugar de trabajo? (selección múltiple)

Preventivo ○ Correctivo ○ Ninguno ○ No sabe ○

6.4. **Anexo 4:** Nivel de significancia y grados de libertad

Nivel de significancia:

En estadística, se define como la probabilidad de aceptar la hipótesis de trabajo cuando esta es verdadera" (Oleachea, 2006, p.48).

Para este caso se tomó un nivel de significancia de 95% y con un porcentaje de error del 5%, el cual se consideró por las siguientes razones:

- Por el cálculo de la muestra poblacional
- Por el establecimiento de hipótesis y operacionalización de las mismas
- La aleatoriedad sobre el proceso de recolección de información
- Por el vaciado de información.

Grados de libertad:

"En estadística, grados de libertad de un estadístico calculado en base a "n" datos, se refiere al número de cantidades independientes que se necesitan en su cálculo, menos el número de restricciones que ligan a las observaciones y el estadístico"(Oleachea, 2006, p. 34).

Por el proceso que se realizó sobre la muestra poblacional se estableció los grados de libertad como **v=1**, ya que sólo se extrajo una muestra de la población y la misma no tiene relación con otra muestra.

6.5. Anexo 5: Tablas de contingencia utilizadas en la comprobación de las hipótesis

Hipótesis 1

Variable independiente: Usuarios no capacitados

Recursos económicos

Tiempo laboral de capacitaciones * Inversión de presupuesto en aspectos para mejorar la seguridad de información

		Inversión de presupuesto en aspectos para mejorar la seguridad de información			Total
		Si	No	No sabe	
Tiempo laboral de capacitaciones	Si	9	7	3	19
	No	12	42	9	63
	No sabe	1	1	0	2
Total		**22**	**50**	**12**	**84**

Fuente: Programa SPSS

Conocimientos de informática

En la tabla de contingencia que se muestra a continuación, para la pregunta *"Tiempo en el que reciben actualización sobre seguridad",* para efectos de análisis se agrupo las respuestas en dos categorías, debido a que fue una pregunta de opciones múltiples y para el análisis únicamente se necesitó conocer si las instituciones estaban recibiendo capacitaciones o no, distribuyendo las opciones de la siguiente manera:

Si = Mensual, Semestral, Anual

No = No recibe

Condición de políticas en la institución * Tiempo en el que reciben actualización sobre seguridad

		Tiempo en el que reciben actualización sobre seguridad		Total
		Si	No	
Condición de políticas en la institución	No se tienen políticas de seguridad definidas	4	47	51
	Actualmente se encuentran en desarrollo	7	5	12
	Política formal, no implementada	2	4	6
	Política formal, escrita e informada al personal	6	2	8
	No sabe	0	7	7
Total		**19**	**65**	**84**

Fuente: Programa SPSS

Disponibilidad de tiempo

Tiempo laboral de capacitaciones * Tiempo en el que reciben actualización sobre seguridad

		Tiempo en el que reciben actualización sobre seguridad			Total
		Anual	Semestral	No recibe	
Tiempo laboral de capacitaciones	Si	13	6	0	19
	No	0	0	63	63
	No sabe	0	0	2	2
Total		**13**	**6**	**65**	**84**

Fuente: Programa SPSS

Variable dependiente: Poca seguridad sobre la información que manejan.

Políticas de seguridad implementadas

En la tabla de contingencia que se muestra a continuación, para la pregunta *"*Asistencia técnica recibida*",* para efectos de análisis se agruparon las respuestas en dos categorías, debido a que fue una pregunta de opciones múltiples y para el análisis únicamente se necesitó conocer si las instituciones contaban con un especialista que les brinde asistencia técnica local o no, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Técnico local

No = Técnicos de sede central, Técnicos por contrato temporal, no recibe asistencia técnica.

Para la pregunta *"*Condición de políticas en la institución*",* se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó conocer si las instituciones estaban implementando políticas de seguridad informática o no, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Política formal, escrita documentada e informada a todo el personal

No= No se tienen políticas de seguridad definidas, Actualmente se encuentran en desarrollo, Política formal no implementada, No sabe.

Asistencia técnica recibida * Condición de políticas en la institución

		Condición de políticas en la institución			Total
		Implementadas	No implementadas	No sabe	
Asistencia técnica recibida	Si	3	7	0	10
	No	7	54	6	67
	No sabe	1	5	1	7
Total		**11**	**66**	**7**	**84**

Fuente: Programa SPSS

Uso inadecuado de herramientas o equipo

En la tabla de contingencia que se muestra a continuación, para la pregunta "uso de herramientas de descargas", se agruparon las respuestas en dos categorías, debido a que es una pregunta de opciones múltiples y para el análisis únicamente se necesitó conocer si las instituciones estaban utilizando herramientas de descargas, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Skype, Atube Catcher, Ares, Emule, Otros.

No = Ninguno.

Para la pregunta "Problemas de seguridad informática lógica", para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó conocer si las instituciones habían tenido problemas de seguridad lógica, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Intrusos informáticos, hurto de contraseña, alteración de datos, robo de información, virus, otros.

No = Ninguno.

No sabe = No sabe

Problemas de seguridad informática lógica * Uso de herramientas de descargas

		Uso de herramientas de descargas		Total
		Si	No	
Problemas de seguridad informática lógica	Si	32	38	70
	No	5	6	11
	No sabe	0	3	3
Total		**37**	**47**	**84**

Fuente: Programa SPSS

Hipótesis 2

Variable independiente: Falta de aplicación de medidas de seguridad lógica

Falta de conocimiento

En la tabla de contingencia que se muestra a continuación, para la pregunta *"*Asistencia técnica recibida*",* para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó conocer si las instituciones contaban con un especialista que les brinde asistencia técnica local o no, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Técnico local

No = Técnicos de sede central, Técnicos por contrato temporal, no recibe asistencia técnica.

Asistencia técnica recibida * Capacitación cuando hay actualizaciones del sistema

		Capacitación cuando hay actualizaciones del sistema			Total
		Si	No	No sabe	
Asistencia técnica recibida	Si	4	6	0	10
	No	22	41	4	67
	No sabe	3	4	0	7
Total		**29**	**51**	**4**	**84**

Fuente: Programa SPSS

Tipo de información manejada

Evaluación de la seguridad * Tipo de información manejada

		Tipo de información manejada			Total
		Pública	Privada	Ambos	
Evaluación de la seguridad	Si	1	22	5	28
	No	6	37	11	54
	No sabe	0	2	0	2
Total		7	61	16	84

Fuente: Programa SPSS

Contraseña

Tipo de información manejada * Uso de contraseña

		Uso de contraseña		Total
		Si	No	
Tipo de información manejada	Pública	6	1	7
	Privada	53	8	61
	Ambos	9	7	16
Total		**68**	**16**	**84**

Fuente: Programa SPSS

Variable dependiente: Pérdida de información de las instituciones

Amenazas más comunes

En la tabla de contingencia que se muestra a continuación, para la pregunta *"*Problemas de seguridad informática lógica" se agruparon las respuestas en dos categorías, debido a que es una pregunta de opciones múltiples y para el análisis únicamente se necesitó conocer si las instituciones habían tenido problemas relacionados con la seguridad lógica, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Alteración de los datos, virus, Hurto de contraseña, Intrusos informáticos.

No= Ninguno.

Para la pregunta "Uso de herramientas de descargas", para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó conocer si las instituciones estaban utilizando herramientas de descarga o no, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Skype, Atube cátcher, Emule, Ares, Otros.

No = Ninguno

Uso de herramientas de descargas * Problemas de seguridad informática lógica

		Problemas de seguridad informática lógica			Total
		Si	No	No sabe	
Uso de herramientas de descargas	Si	32	5	0	37
	No	38	6	3	47
Total		**70**	**11**	**3**	**84**

Fuente: Programa SPSS

Copias de seguridad

En la tabla de contingencia que se muestra a continuación, para la pregunta "Realización de respaldos" se agruparon las respuestas en dos categorías, debido a que es una pregunta de opciones múltiples y para el análisis únicamente se necesitó conocer si las instituciones realizaban respaldos de seguridad de la información y esto se puedo identificar por medio de las instituciones que seleccionaron uno o más medios de almacenamiento de copias de seguridad, en el instrumento utilizado para la recolección de la información, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Respaldo en discos duros, Respaldos en CD, Respaldos en USB, Otros.

No= Ninguno.

Tipo de información manejada * Realización de respaldos

		Realización de respaldos			Total
		Si	No	No sabe	
Tipo de información manejada	Pública	6	0	1	7
	Privada	56	4	1	61
	Ambos	12	1	3	16
Total		74	5	5	84

Fuente: Programa SPSS

Antivirus

En la tabla de contingencia que se muestra a continuación, para la pregunta “Problemas de seguridad informática lógica” se agruparon las respuestas en dos categorías, debido a que es una pregunta de opciones múltiples y para el análisis únicamente se necesitó conocer si las instituciones habían tenido problemas relacionados con la seguridad lógica, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Alteración de los datos, virus, hurto de contraseña, intrusos informáticos.

No= Ninguno.

No sabe = No sabe

Problemas de seguridad informática lógica * Tipo de antivirus

		Tipo de antivirus				Total
		Gratuita	Pagada	No se cuenta con antivirus	No sabe	
Problemas de seguridad informática lógica	Si	28	31	3	8	70
	No	2	3	0	6	11
	No sabe	2	0	0	1	3
Total		**32**	**34**	**3**	**15**	**84**

Fuente: Programa SPSS

Hipótesis 3

Variable independiente: Falta de un área informática.

Falta de recursos económicos

Departamento interno * Recursos económicos

		Recursos económicos			Total
		Si	No	No sabe	
Departamento interno	Si	6	2	1	9
	No	19	53	3	75
Total		**25**	**55**	**4**	**84**

Fuente: Programa SPSS

Asistencia técnica externa

Departamento interno * Asistencia técnica recibida

		Asistencia técnica recibida					Total
		Técnicos de sedes centrales	Técnicos locales	Técnicos por contrato temporal	No recibo asistencia	No sabe	
Departamento interno	Si	0	7	0	0	2	9
	No	39	3	24	4	5	75
Total		**39**	**10**	**24**	**4**	**7**	**84**

Fuente: Programa SPSS

Variable dependiente: No se brinda asistencia técnica inmediata.

Equipo adecuado

En la tabla de contingencia que se muestra a continuación, para la pregunta *"*Recibe asistencia técnica inmediata*",* para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó conocer si las instituciones reciben asistencia técnica inmediata, distribuyendo las opciones de respuesta de la siguiente manera:

Si = inmediatamente

No = De 1 a 5 días, De 6 a 15 días, de 16 a 30 días, más de 30 días.

Recibe mantenimiento inmediato * Herramientas para mantenimiento

		Herramientas para mantenimiento			Total
		Si	No	No sabe	
Recibe asistencia técnica inmediata	Si	9	16	0	25
	No	4	50	3	57
	No sabe	0	2	0	2
Total		**13**	**68**	**3**	**84**

Fuente: Programa SPSS

Personal no capacitado

En la tabla de contingencia que se muestra a continuación, para la pregunta "Asistencia técnica recibida", para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó conocer si las instituciones cuentan con un especialista que les brinde asistencia técnica local o no, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Técnico local

No = Técnicos de sede central, Técnicos por contrato temporal, no recibe asistencia técnica.

Para la pregunta "Tiempo en el que reciben actualización sobre seguridad", para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó conocer si las instituciones se actualizaban sobre seguridad informática, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Mensual, Semestral, Anual

No = No recibe

Tiempo en el que reciben actualización sobre seguridad * Asistencia técnica recibida

		Asistencia técnica recibida			Total
		Si	No	No sabe	
Tiempo en el que reciben actualización sobre seguridad	Si	3	14	2	19
	No	7	53	5	65
Total		**10**	**67**	**7**	**84**

Fuente: Programa SPSS

Accesibilidad

En la tabla de contingencia que se muestra a continuación, para la pregunta *"*Asistencia técnica recibida*",* para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó conocer si las instituciones contaban con un especialista que les brinde asistencia técnica local o no, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Técnico local

No = Técnicos de sede central, Técnicos por contrato temporal, no recibe asistencia técnica.

Asistencia técnica recibida * Tiempo de asistencia técnica

		Tiempo de asistencia técnica						Total
		Inmediatamente	De 1 a 5 días	De 6 a 15 días	De 16 a 30 días	No recibe asistencia	No sabe	
Asistencia técnica recibida	Si	6	4	0	0	0	0	10
	No	17	35	4	3	6	2	67
	No sabe	2	4	0	1	0	0	7
Total		**25**	**43**	**4**	**4**	**6**	**2**	**84**

Fuente: Programa SPSS

Hipótesis 4

Variable independiente: Riesgos físicos

Infraestructura

En la tabla de contingencia que se muestra a continuación, para la pregunta “Problemas de infraestructura”, para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó conocer si las instituciones tenían o no problemas de infraestructura, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Mala ubicación de tomacorrientes, Infiltración de agua, Tomacorrientes insuficientes, Ventilación inapropiada, Poco espacio

No = Ninguno.

No sabe = No sabe

Para la pregunta “Razones que afectan el buen funcionamiento de equipo”, para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó conocer si existían razones que hubieran afectado el buen funcionamiento del equipo informático de las instituciones, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Falta de limpieza rutinaria, mala ubicación del equipo, espacio reducido para la ubicación del equipo, falta de aire acondicionado, chispazos eléctricos en los tomacorrientes, otras.

No = Ninguno

Razones que afectan el buen funcionamiento de equipo * Problemas de infraestructura

		Problemas de infraestructura			Total
		Si	No	No sabe	
Razones que afectan el buen funcionamiento de equipo	Si	54	14	4	72
	No	5	6	1	12
Total		**59**	**20**	**5**	**84**

Fuente: Programa SPSS

Sobrecalentamiento del equipo

En la tabla de contingencia que se muestra a continuación, para la pregunta *“Razones que provocan sobrecalentamiento al equipo”* para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se utilizaron las diferentes

razones que pueden ser factores para que el equipo sufriera sobrecalentamiento, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Falta de aire acondicionado, falta de limpieza rutinaria.

No = Espacio reducido para ubicar el equipo, Chispazos eléctricos en tomacorrientes, Mala ubicación del equipo.

Razones que provocan sobrecalentamiento al equipo * Problemas de sobrecalentamiento

		Problemas de sobrecalentamiento			Total
		Si	No	No sabe	
Razones que provocan sobrecalentamiento al equipo	Si	31	27	4	62
	No	0	22	0	22
Total		31	49	4	**84**

Fuente: Programa SPSS

Delincuencia

Equipo expuesto a la afluencia de personas * Casos de robo

		Casos de robo			Total
		Si	No	No sabe	
Equipo expuesto a la afluencia de personas	Si	0	10	0	10
	No	8	63	3	74
Total		8	73	3	**84**

Fuente: Programa SPSS

Variable Dependiente: Vulnerabilidad del equipo informático.

Vida útil

Tiempo de uso de la computadora

Opciones	Frecuencia	Porcentaje
Menos de 1 año	12	14.3%
De 1 a 2 años	21	25.0%
De 3 a 5 años	28	33.3%
Más de 5 años	23	27.4%
Total	**84**	**100.0%**

Fuente: Programa SPSS

Acondicionamiento

En la tabla de contingencia que se muestra a continuación, para la pregunta *"Razones que provocan sobrecalentamiento al equipo"* para efectos de análisis se agrupo las respuestas en dos categorías, ya que para el análisis únicamente se utilizaron las diferentes razones que podían ser factores para que el equipo sufriera de sobrecalentamiento, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Falta de aire acondicionado, falta de limpieza rutinaria.

No = Espacio reducido para ubicar el equipo, Chispazos eléctricos en tomacorrientes, Mala ubicación del equipo.

Para la pregunta *"*Fallos de rendimiento*"* para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó saber si los equipos de las instituciones estaban presentando fallos de rendimiento o no, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Lentitud, Congelamiento de pantallas, Apagones.

No = Ninguno.

Fallos de rendimiento * Razones que provocan sobrecalentamiento al equipo

		Razones que provocan sobrecalentamiento al equipo		Total
		Si	No	
Fallos de rendimiento	Si	52	12	64
	No	10	10	20
Total		**62**	**22**	**84**

Fuente: Programa SPSS

Ubicación

En la tabla siguiente, las opciones de respuesta para la interrogante "infraestructura que afecta la ubicación del equipo" se distribuyeron de la siguiente manera:

Si = Mala ubicación de tomacorrientes, Tomacorrientes insuficientes, Poco espacio

No = Ninguno, Infiltración de agua, Ventilación inapropiada.

Infraestructura que afecta la ubicación del equipo

Opciones	Frecuencia	Porcentaje
Si	43	51.2
No	36	42.9
No sabe	5	6.0
Total	**84**	**100.0%**

Fuente: Programa SPSS

Capacidad

En la tabla de contingencia que se muestra a continuación, para la pregunta "Fallos de rendimiento" se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó saber si los equipos de las instituciones estaban presentando fallos de rendimiento o no, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Lentitud, Congelamiento de pantallas, Apagones.

No = Ninguno.

Tiempo de uso de la computadora * Fallos de rendimiento

		Fallos de rendimiento		Total
		Si	No	
Tiempo de uso de la computadora	Menos de 1 año	7	5	12
	De 1 a 2 años	17	4	21
	De 3 a 5 años	22	6	28
	Más de 5 años	18	5	23
Total		64	20	84

Fuente: Programa SPSS

Mantenimiento al equipo

En la tabla de contingencia que se muestra a continuación, para la pregunta "Razones que provocan sobrecalentamiento al equipo" para efectos de análisis se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se utilizaron las diferentes razones que podían ser factores para que el equipo sufriera de sobrecalentamiento, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Falta de aire acondicionado, falta de limpieza rutinaria.

No = Espacio reducido para ubicar el equipo, Chispazos eléctricos en tomacorrientes, Mala ubicación del equipo.

Para la pregunta *"Fallos de rendimiento"* se agruparon las respuestas en dos categorías, ya que para el análisis únicamente se necesitó saber si los equipos de las instituciones estaban presentando fallos de rendimiento o no, distribuyendo las opciones de respuesta de la siguiente manera:

Si = Lentitud, Congelamiento de pantallas, Apagones.

No = Ninguno.

Fallos de rendimiento * Se efectúa mantenimiento preventivo

		Razones que provocan sobrecalentamiento al equipo		Total
		Si	No	
Fallos de rendimiento	Si	28	36	64
	No	12	8	20
Total		**40**	**44**	**84**

Fuente: Programa SPSS

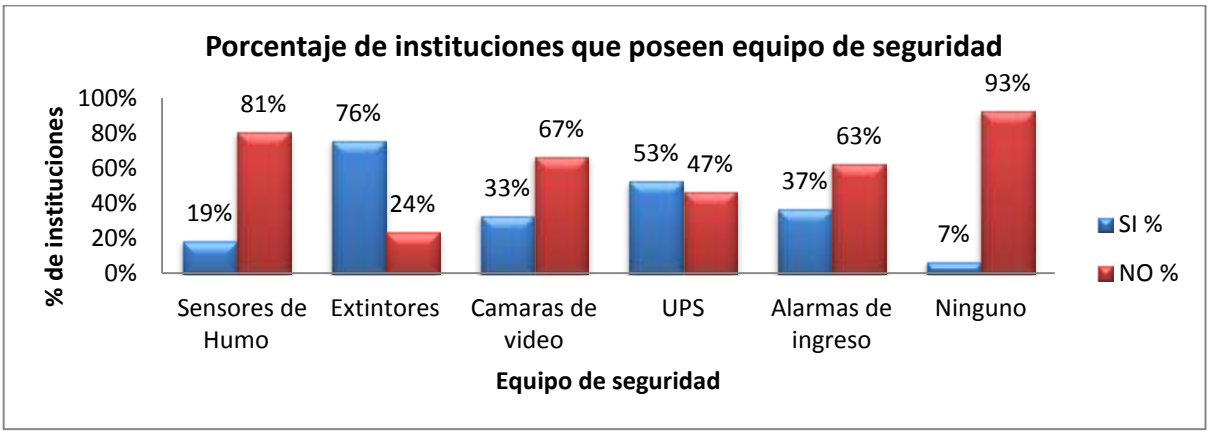
6.6. Anexo 6: Datos utilizados en el diagnóstico de vulnerabilidades.

Equipo de seguridad con que contaban las instituciones

Equipo de seguridad	SI	SI %	NO	NO %
Sensores de Humo	21	19%	87	81%
Extintores	82	76%	26	24%
Cámaras de video	36	33%	72	67%
UPS	57	53%	51	47%
Alarmas de ingreso	40	37%	68	63%
Ninguno	8	7%	100	93%

Fuente: Elaboración propia

Gráfica 1



Fuente: Elaboración propia

Instituciones que contaban con aire acondicionado

Aire acondicionado	Instituciones	%
Si	55	51 %
No	46	43%
Algunos	7	6%

Fuente: Elaboración propia

Gráfica 2

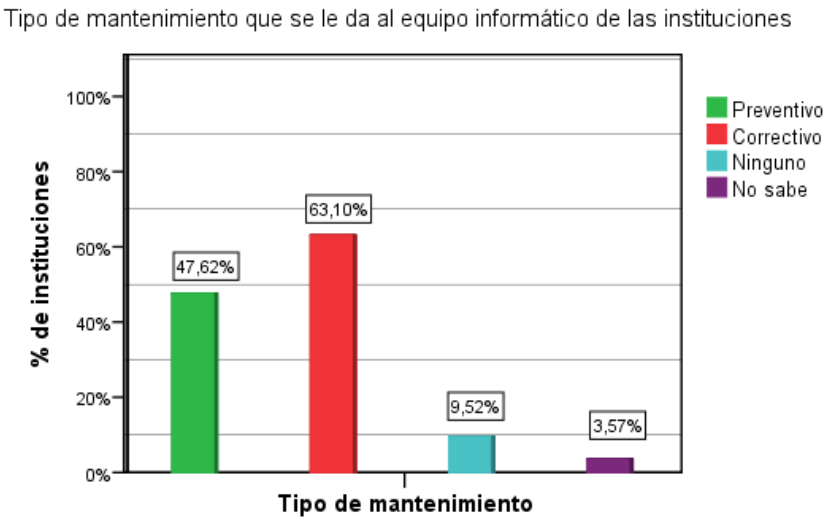
Fuente: Elaboración propia

Mantenimiento al equipo informático

Opciones	Respuestas		Porcentaje de casos
	N°	Porcentaje	
Preventivo	40	38.5%	47.6%
Correctivo	53	51.0%	63.1%
Ninguno	8	7.7%	9.5%
No sabe	3	2.9%	3.6%
Total	104	100.0%	123.8%

Fuente: Elaboración propia

Grafica 3



Fuente: Elaboración propia

Consumo de alimentos mientras se trabaja en la computadora

Consume alimentos	Instituciones	%
SI	25	23%
NO	83	77%

Fuente: Elaboración propia

Gráfica 4

Fuente: Elaboración propia

Instituciones con espacio suficiente para ubicar el equipo

Espacio suficiente	Instituciones	%
SI	72	67%
NO	36	33%

Fuente: Elaboración propia

Grafica 5

Fuente: Elaboración propia

Instituciones que contaban con sistema informático

Sistema Informático	Instituciones	%
SI	108	100%
NO	0	0%

Fuente: Elaboración propia

Gráfica 6

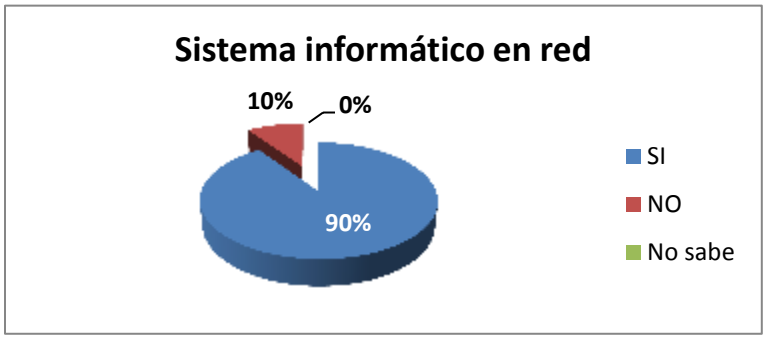
Fuente: Elaboración propia

Instituciones que tenían el sistema informático en red

Sistema Informático en red	Instituciones	%
SI	108	100%
NO	0	0%

Fuente: Elaboración propia

Gráfica 7



Fuente: Elaboración propia

Instituciones que poseían antivirus

Antivirus	Instituciones	%
SI	93	86%
NO	12	11%
No sabe	3	3%

Fuente: Elaboración propia

Gráfica 8

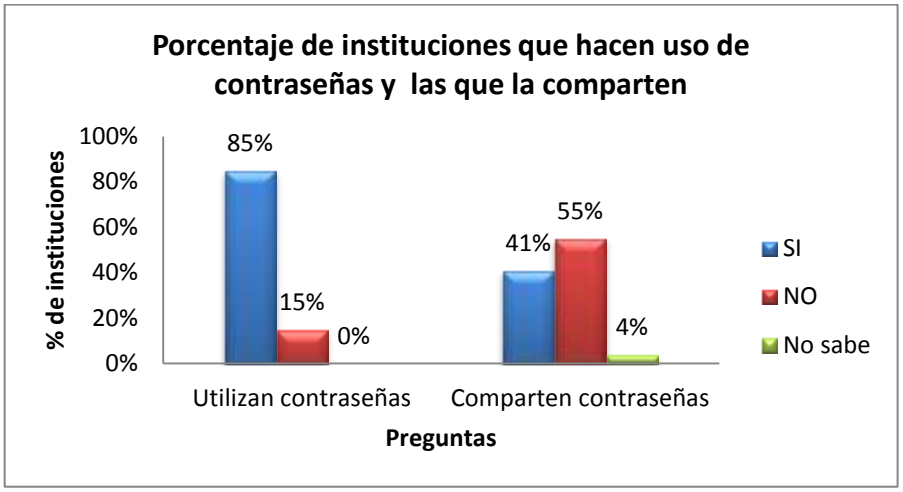
Fuente: Elaboración propia

Instituciones que hacían uso de contraseñas para acceder a la información

Se utiliza contraseña	Utilizan contraseñas	% que utilizan	Comparten contraseñas	% que comparten
SI	92	85%	38	41%
NO	16	15%	50	55%
No sabe	0	0%	4	4%

Fuente: Elaboración propia

Gráfica 9



Fuente: Elaboración propia

Copias de seguridad

Copias de Seguridad	Instituciones	%
Si	69	64%
No	37	34%
No sabe	2	2%

Fuente: Elaboración propia

Gráfica 10

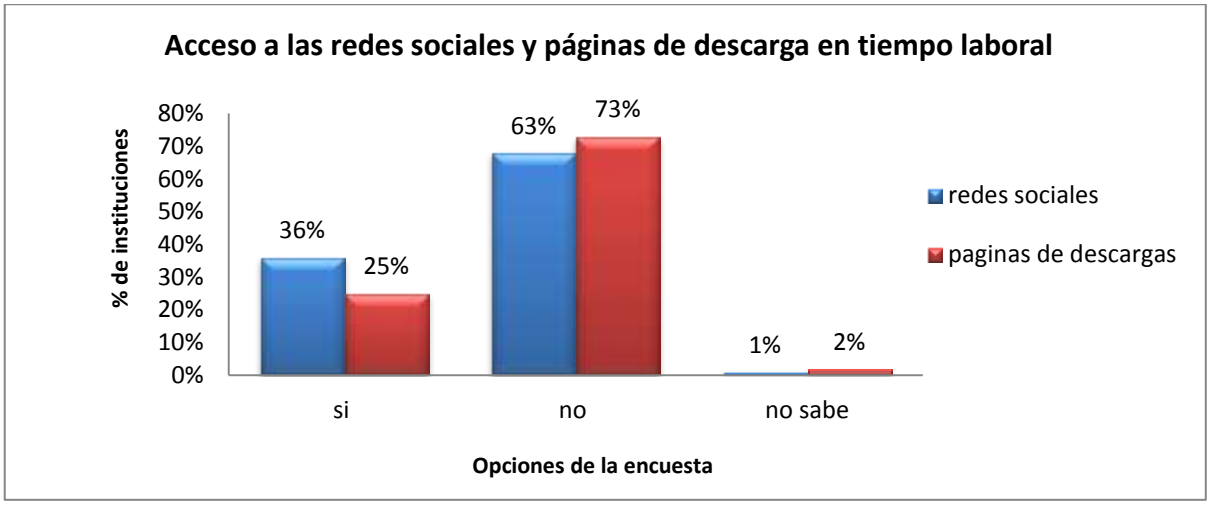
Fuente: Elaboración propia

Instituciones con accesos a páginas de descarga y redes sociales

Opciones de cuestionario	Redes sociales	%	Páginas de descargas	%
SI	39	36%	27	25%
NO	68	63%	79	73%
No sabe	1	1%	2	2%

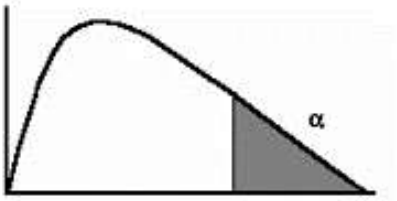
Fuente: Elaboración propia

Gráfica 11



Fuente: Elaboración propia

6.7. Anexo 7: Tabla de la distribución ji cuadrada (X^2).



Grados de libertad	α=.995	α=.99	α=.975	α=.95	α=.90	α=.10	α=.05	α=.025	α=.01	α=.005
1	0.0000	0.0002	0.0010	0.0039	0.0158	2.7055	3.8415	5.0239	6.6349	7.8794
2	0.0100	0.0201	0.0506	0.1026	0.2107	4.6052	5.9915	7.3778	9.2103	10.597
3	0.0717	0.1148	0.2158	0.3518	0.5844	6.2514	7.8147	9.3484	11.345	12.838
4	0.2070	0.2971	0.4844	0.7107	1.0636	7.7794	9.4877	11.143	13.277	14.860
5	0.4117	0.5543	0.8312	1.1455	1.6103	9.2364	11.070	12.833	15.086	16.750
6	0.6757	0.8721	1.2373	1.6354	2.2041	10.645	12.592	14.449	16.812	18.548
7	0.9893	1.2390	1.6899	2.1673	2.8331	12.017	14.067	16.013	18.475	20.278
8	1.3444	1.6465	2.1797	2.7326	3.4895	13.362	15.507	17.535	20.090	21.955
9	1.7349	2.0879	2.7004	3.3251	4.1682	14.684	16.919	19.023	21.666	23.589

6.8. Anexo 8: Reporte que muestra el software desarrollado

REPORTE DEL NIVEL DE SEGURIDAD DE BASES DE DATOS Y REDES INFORMATICAS

REPORTE GENERAL

EMPRESA UES

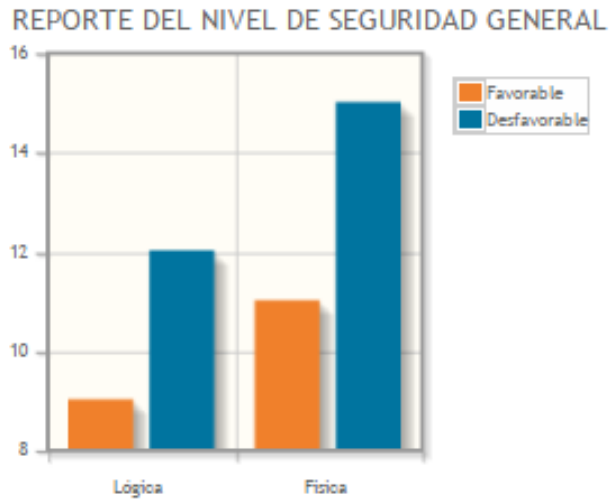
Fecha de reporte: **13-03-2015**

Test realizado: **12-03-15**

Reporte de nivel de seguridad General

La empresa muestra los siguientes resultados en cuanto a seguridad de bases de datos y redes informáticas:

Sub-área	Favorable	Desfavorable	Total por área	Nivel de seguridad
Seguridad lógica	9	12	21	Medio
Seguridad física	11	15	26	Bajo
Total evaluación	20	27	47	



REPORTE DE RECOMENDACIONES DE SEGURIDAD

EMPRESA UES

Fecha de reporte: 13-11-2014
Test realizado: 12-08-14
Reporte de: Recomendaciones generales

Se sugiere a la empresa poner en práctica las siguientes recomendaciones con respecto a la seguridad de bases de datos y redes informáticas correspondiente a las áreas de seguridad física y lógica:

Seguridad física

Recomendaciones para infraestructura

Recomendaciones para el hardware

Recomendaciones para el uso de medios de almacenamiento

Seguridad Lógica

Recomendaciones para el acceso a la información

Recomendaciones para el uso de la información

6.9. Anexo 9: Presupuesto

Recurso humano

Se detallan los gastos necesarios de recurso humano para la realización de la investigación y para el desarrollo del software.

Recurso humano en investigación y diagnóstico

Cargo	Cantidad	Meses	Salario Mensual en ($)	Totales en ($)
Investigador[3]	3	6	300.00	**5,400.00**

Fuente: Elaboración propia

Recurso humano para etapa de desarrollo

Cargo	Cantidad	Meses	Salario Mensual en ($)	Sub totales en ($)
Analista[4]	3	1	800	2,400
Diseñador[5]	3	1	400	1,200
Programador[6]	3	4	350	4,200
Total				**7,800**

Fuente: Elaboración propia

Recursos materiales

Se consideran los bienes que fueron necesarios para alcanzar el logro de los objetivos entre ellos podemos encontrar los siguientes elementos: Papelería y útiles, costo de energía, costo de servicio de internet, costos de transporte y de presentación.

[3] Los salarios considerados fueron obtenidos del sitio web un mejor empleo. Recuperado de http:// www.sv.unmejorempleo.com/ busqueda_resultados.php
[4] Ibid.
[5] Ibid.
[6] Ibid.

Papelería y útiles

Descripción	Precio unitario en ($)	Cantidad	Sub totales en ($)
Resmas de papel bond Tamaño carta	4.00	7	28.00
Folders	0.20	35	7.00
Faster	0.10	35	3.5
Lapiceros	0.20	3	0.60
Lápices	0.15	6	0.90
Copias	0.02	2000	40.00
Tinta negra 1L	7.00	1	7.00
Tinta de color 1/2L(Amarilla, Azul, magenta)	5.80	3	17.40
Anillados	1.50	5	7.50
DVD	0.75	4	3.00
CD	0.50	6	3.00
Portada para CD	1.50	6	9.00
Empastado de lujo	15	4	60.00
Caja de grapas	2.00	1	2.00
Total			**188.90**

Fuente: Elaboración propia

Costo de energía eléctrica

Cargo	Valor en ($)
Cargo por comercialización	0.97
Cargo por energía	32.64
Cargo por distribución	5.13
Estimación del cargo mensual	38.74
Estimación del cargo Anual	**464.88**

Fuente: Simulador CAESS[7]

Para el costo de internet se consideró cubrir el servicio de internet con una velocidad 512 MB durante el desarrollo del proyecto. Ver tabla siguiente

Costo de servicio de internet

Descripción	Precio Unitario en ($)	Meses	Total ($)
Servicio de Internet[8]	13.99	12	**167.88**

Fuente: Elaboración propia

[7] El valor de la energía fue obtenido del Simulador de Consumo Eléctrico Residencial de CAESS. Recuperado de http:// www.aeselsalvador.com/ simulador/ Simulador2.html

[8] Para el costo de internet se considera la tarifa cobrada por la empresa Claro. Recuperado de http://www.claro.com.sv/ wps/portal/sv/ pc/personas/internet/ internet-residencial

Gastos de transporte

Son los gastos promedio en que se incurriría para poder trasportarse hacia los puntos de salidas de campo (ver tabla 21).

Costo de transporte colectivo en promedio por persona =$1.50 por día

Días de trabajo de campo = 22

Costo de transporte colectivo = (1.50*22) = $33 por persona

Gastos de transporte

Descripción	Número de personas	Costo total por persona en ($)	Sub-total en ($)
Transporte colectivo	3	33	**99.00**

Fuente: Elaboración propia

Gastos de presentación

Se consideran los gastos que fueron necesarios para poder ambientar la sala de presentaciones donde se desarrollarían las defensas de cada una de las tres etapas del proyecto de tesis. Ver tabla siguiente:

Gastos de presentación

Descripción	Cantidad	Precio unitario en ($)	Total en ($)
Botellas de Agua	10	0.50	5.00
Refrigerio (De las tres etapas)	50	1	50
Flores	1	15	15
Total			**70.00**

Fuente: Elaboración propia

Recursos lógicos

En los recursos lógicos se consideraron los recursos intangibles necesarios para poder llevar a cabo el desarrollo del proyecto. Ver tabla siguiente.

Gastos de software

Licencia de Software	Cantidad	Precio Unitario en ($)
Microsoft Project 2010[9]	1	600.00
PSPP	1	0.0
MySql	1	0.0
Sk1 Project	1	0.0
Notepad++	1	0.0
Total		**600.00**

Fuente: Elaboración propia

Costos totales del proyecto

Se muestra el resumen de todos los costos incurridos para poder desarrollar el proyecto. Ver tabla siguiente.

[9] El precio considerado para MicrosoftProject2010 fue el establecido por la empresa MicrosoftStore en su página web. Recuperado de www.microsoftstore.com/store/msstore/en_US/pd/Project-2010-Spanish/productID.216566600

GLOSARIO

Administrador informático: Persona que administra y tiene a su cargo el área informática de una institución.

Backup: Se utiliza para tener una o más copias de información considerada importante y así poder recuperarla en el caso de pérdida de la copia original

Banda magnética: Es un tipo de medio o soporte de almacenamiento de datos que se graba en pistas sobre una banda plástica con un material magnetizado, generalmente óxido de hierro.

Base de datos: Conjunto de datos almacenados y organizados con el fin de facilitar su acceso y recuperación mediante un ordenador.

Contraseña: Conjunto finito de caracteres limitados que forman una palabra secreta que sirve a uno o más usuarios para acceder a un determinado recurso.

Datos: Representación simbólica de un atributo de una entidad ya se numérica o alfanumérica.

Estrategia: Técnica y conjunto de actividades destinadas a conseguir un objetivo.

Fichas bibliográficas: Son aquellas tarjetas que describen los datos de libros y documentos monográficos.

Fichas hemerográficas: Son aquellas tarjetas que describen artículos de revistas o periódicos.

Hardware: Conjunto de elementos materiales que constituyen el soporte físico de un ordenador.

Hipótesis: Suposición sin pruebas que se toma como base de un razonamiento.

Ibid.: Que significa en el mismo lugar, se utiliza si la obra se cita dos o más veces consecutivas.

Institución pública: Organismo que desempeña una función de interés público, especialmente educativa o del gobierno.

Lahar: Es un flujo de sedimento y agua que se moviliza desde las laderas de volcanes.

Medidas Correctivas: Es una actuación o efecto implementado a eliminar las causas de una inconformidad, defecto, o situación indeseable detectada con el fin de evitar su repetición.

Medidas preventivas: Es la acción y efecto de prevenir o preparar con anticipación lo necesario para un fin, anticiparse a una dificultad, prever un daño.

Op cit.: Que significa en la obra citada y se usa cuando se cita de nuevo una obra que se ha referenciado de manera completa pero no en la referencia inmediatamente anterior.

Protocolo: Conjunto de normas y procedimientos útiles para la transmisión de datos, conocido por el emisor y el receptor.

Redes informáticas: Conexión simultánea de distintos equipos informáticos a un sistema principal.

Riesgo: Proximidad de un daño o peligro.

Seguridad: Mecanismo que relaciona diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

Software: Término genérico que se aplica a los componentes lógicos de un sistema informático, como por ej. Los programas, sistemas operativos, que permiten a este ejecutar sus tareas.

UPS: Fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.

Virus: Programa que se incorpora a un ordenador a través de sistemas de comunicación, y que se ejecuta automáticamente en determinados momentos modificando o destruyendo los datos contenidos en el ordenador.

Vulnerabilidad: Puntos débiles del equipamiento, aplicaciones, personal y mecanismos de control que facilitan la concreción de una amenaza.

Antivirus: en informática los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos.

Anti- spyware: Es un programa desarrollado para el ámbito de la seguridad informática, el cual protege a los usuarios de programas maliciosos.

Criptografía: es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

Encriptación: es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible esta no pueda ser obtenida con facilidad por terceros.

Firewall: es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Informática: es una ciencia que estudia métodos, procesos, técnicas, con el fin de almacenar, procesar y transmitir información y datos en formato digital.

Políticas de seguridad: es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información bajo el punto de vista de cierta entidad.

Picos de potencia: máxima potencia eléctrica que se puede generar.

Transmisión de datos: es la transferencia física de datos por un canal de comunicación.

Laravel: es un framework de código abierto para desarrollar aplicaciones y servicios web con PHP 5. Su filosofía es desarrollar código PHP de forma elegante y simple, para crear código de forma sencilla y permitiendo multitud de funcionalidades. Intenta aprovechar lo mejor de otros frameworks y aprovechar las características de las últimas versiones de PHP.

Modelo: Los modelos son clases encargadas de trabajar con las consultas de la base de datos, es decir que por cada tabla tendremos una clase, cada registro será un objeto y las consultas se llamarán a través de métodos de esas clases. A su vez laravel trabaja con Eloquent que es un ORM que nos facilitará el trabajo de las consultas a través de métodos ya establecidos, estos nos permitirán realizar las tareas más comunes y que más se repiten en una base de datos como insertar, recuperar registros por su id, modificar esos registros, listarlos, eliminarlos

ORM: Es una técnica de programación para convertir datos entre el sistema de tipos utilizado en un lenguaje de programación orientado a objetos y la utilización de una base de datos relacional.

Vista: La vista es la parte visual de la aplicación, estas se encuentran incluidas en laravel como un paquete de procesamiento de plantillas llamado Blade. Este sistema de plantillas favorece un código mucho más limpio ya que evita la combinación de código html y PHP en las vistas.

Controlador: Los controladores son clases con métodos, también llamados acciones, estas acciones se comunicarán con los modelos para hacer consultas a la base de datos, y con las vistas para devolver una respuesta al cliente, los controladores contienen la lógica de la aplicación y permiten organizar el código en clases.

Clase: Una clase es una plantilla para la creación de objetos de datos según un modelo predefinido. Las clases se utilizan para representar entidades o conceptos. Cada clase es un modelo que define un conjunto de variables y métodos apropiados para operar con dichos datos. Cada objeto creado a partir de la clase se denomina instancia de la clase.

Objetos: Es la instancia de una clase, entidad provista de un conjunto de propiedades o atributos (datos) y de comportamiento o funcionalidad (métodos), los mismos que consecuentemente reaccionan a eventos. Se corresponden con los objetos reales del mundo que nos rodea, o con objetos internos del sistema (del programa). Es una instancia a una clase.