UNIVERSIDAD NACIONAL
“SAN LUIS GONZAGA DE ICA”

FACULTAD DE INGENIERÍA DE SISTEMAS

TEMA

“Modelo de un Sistema de Seguridad Informática Aplicado en la Empresa Municipal de Agua Potable y Alcantarillado de Ica - EMAPICA”

PARA OPTAR EL TITULO DE PROFESIONAL DE:

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER:

ESTUARDO ALEXANDER, HUAMAN NAVARRO

ASESOR: Magister Selene Pineda Morán

ICA – PERU

2018

DEDICATORIA:

Quiero dedicarle esta tesis a mis padres, por el apoyo incondicional en todo momento, quienes son los únicos forjadores de mi futuro y hacer de mí una persona responsable y profesional.

Estuardo

RESUMEN

Para el presente trabajo de tesis, las pruebas de intrusión consisten en probar los métodos de Seguridad.

Fue fundamental identificar las necesidades de seguridad de una organización para establecer las medidas que permitirán a dicha Institución tener la confiabilidad del caso en sus sistemas de información.

Los resultados de la prueba no paramétrica de Wilcoxon para el Indicador 1(Tiempo solicitado para la información) nos demuestra que existe diferencia significativa entre las muestras relacionadas, entre el antes y el después por lo tanto se aprueba la Hipótesis Alterna Ha1. En relación a los resultados de las medias del indicador se tiene que existe una diferencia de 7.93 minutos en favor del Tiempo solicitado para la información, esta diferencia representa una reducción del tiempo de 79.3%.

Asimismo, los resultados de la prueba no paramétrica de Wilcoxon para el indicador 2(Tiempo en crear copia de seguridad de la información) demuestra que existe diferencia significativa entre las muestras relacionadas, entre el antes y el después por lo tanto se aprueba la Hipótesis Alterna Ha1. En relación a los resultados de las medias del indicador se tiene que existe una diferencia de 8.01 minutos en favor del Tiempo en crear copia de seguridad de la información, esta diferencia representa una reducción del tiempo de 80.1%.

Finalmente, podemos concluir que los resultados de la prueba de Wilcoxon, nos arrojan en el indicador 1 una media de 11.88 minutos; con una desviación estándar de la muestra de 1.613 y para el indicador 2, nos arrojan una media de 13.71 minutos; con una desviación estándar de la muestra de 3.857.

INDICE DE CONTENIDOS

INTRODUCCION

En los actuales momentos en que los sistemas de información manejan grandes cantidades de información las instituciones públicas y privadas tienen que poner mucho énfasis en la seguridad con que se debe cautelar dicha información, dado que lo más valioso que tiene una empresa es justamente su información, ya que con ello la competitividad se hace más importante.

Este proceso de investigación acerca de la seguridad informática, debe ser llevado a cabo por un profesional en la auditoria informática, servirá para determinar si en los sistemas que están siendo utilizados por la institución se aplican las medidas de seguridad y de control correspondiente para lograr garantizar la integridad de toda la información que se maneje en el sistema.

La tesis fue desarrollada en 6 capítulos; los cuales paso a detallar:

En el Capítulo I: se desarrolló el marco teórico en donde se planteó los antecedentes, las bases teóricas y el marco conceptual.

En el capítulo II. Se planteó el problema, objetivos e hipótesis donde se desarrolló el planteamiento del problema, la formulación del problema y la delimitación del problema.

En el capítulo III. Se desarrolló la metodología de la investigación, en donde se planteó el tipo de investigación, nivel de investigación, variables e indicadores, la población y la muestra, las técnicas de recolección de información, los instrumentos de recolección de información y las técnicas de análisis e interpretación de datos y resultados.

En el capítulo IV: se planteó el modelo para la seguridad informática, donde se muestra

la seguridad informática, acciones que se tomaran en el planteamiento de la seguridad informática. La seguridad lógica, los niveles de seguridad que se pueden plantear.

En el capítulo V: se desarrolló el análisis e Interpretación de los Resultados para la pre prueba, la contratación de la hipótesis y la discusión de los resultados.

Finalmente en el capítulo VI se desarrollaron las Conclusiones y Recomendaciones

.

CAPITULO I: MARCO TEORICO

1.1. Antecedentes

A. Antecedentes Internacionales.

TITULO: LA AUDITORÍA A LAS TECNOLOGÍAS DE LA INFORMÁTICA. RELACIÓN DEL DERECHO Y LA INFORMÁTICA JURÍDICA

AUTOR: Alcides Francisco Antúnez Sánchez

AÑO: 2013 - Cuba

RESUMEN[1]:

El trabajo recoge un eje temático álgido en su conceptualización y ejecución por los entes y agentes que realizan la auditoría a las tecnologías de la informática o de la información, como a los entes pasivos que son objeto de la misma (personas naturales y jurídicas). Hacemos un recorrido por los comienzos de la actividad de la auditoría en Cuba desde sus inicios tomando como punto de referencia el siglo XX hasta el actual; en relación con la actividad que ejercitan los órganos de control y los organismos de la Administración Pública en Cuba, la base jurídica en que se sustenta la Auditoría a las Tecnologías de la información como auditoría tipo o como complemento de la Auditoría de Sistema dentro de la acción del control gubernamental, hasta la actividad de la Contraloría General de la República. Nos permitió conocer a través de las

[1] https://www.derechoycambiosocial.com/revista032/auditoria_a_las_tecnologias_de_la_informatica.pdf

indisciplinas que existen, que pueden llegar a ser objeto de aplicación de medidas en el orden administrativo-laboral, y del derecho administrativo sancionador y las que corresponden a la responsabilidad penal sí existieren, luego de la revisión y estudio de documentos relacionados con la temática abordada. Aunque en este último aspecto exponemos que la legislación penal en Cuba hay que continuar atemperándola con los actuales tendencias a la comisión de los delitos informáticos, al igual para las figuras contravencionales ya existentes. Palabras claves: auditoría, cibernética, informática jurídica, contraloría.

TITULO: Modelo de auditoría informática para la seguridad física

AUTOR: FLORES YUJRA, ALEJANDRA YMAR

AÑO: 2014 - España

RESUMEN[2]:

El modelo propuesto, obtiene información del nivel de seguridad en la Unidad de Sistemas de la institución. La investigación es un aporte para personas y/o instituciones interesadas en realizar y aplicar una Auditoría a la seguridad física de la información, publicado el 29 septiembre 2014.

[2] http://dialnet.unirioja.es/servlet/oaiart?codigo=2059077

B. Antecedentes Nacionales

TITULO: DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA SERVICIOS POSTALES DEL PERÚ S.A.

AUTOR: David Arturo Aguirre Mollehuanca

AÑO: 2014

RESUMEN[3]:

La exigencia de la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2008 en las entidades públicas nace de la necesidad de gestionar adecuadamente la seguridad de la información en cada una de estas empresas. Sin embargo, el desconocimiento de estos temas por parte de la alta dirección, ha ocasionado que no se tomen las medidas necesarias para asegurar el éxito de este proyecto en el tiempo estimado por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), entidad responsable de apoyar a las entidades públicas durante el proceso de implementación de la norma. Debido a ello, para la realización de este proyecto de fin de carrera, se decidió trabajar con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que pueda, en un futuro, servir

[3] http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5677/AGUIRRE_DAVID_SISTEMA_GESTION_SEGURIDAD_INFORMACION_SERVICIOS_POSTALES.pdf;sequence=1

como referencia para la implementación del mismo. En consecuencia, se realizaron varias reuniones con la alta dirección que permitieran definir el alcance y las políticas del SGSI en la organización enfocándose en los procesos institucionales críticos de dicha entidad, posteriormente se realizó una serie de entrevistas que permitieran identificar y valorar los activos críticos de la organización así como identificar y evaluar los riesgos a los cuales estos estaban sometidos. Por último, se presenta un documento llamado Declaración de Aplicabilidad en el cual se indica que controles de la NTP ISO/IEC 17799:2007 se pueden implementar dentro de la organización basado en el trabajo realizado dentro de la organización.

TITULO: MODELO DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN EN SEGURIDAD, SALUD OCUPACIONAL Y AMBIENTAL PARA LA UNIVERSIDAD RICARDO PALMA APLICADA A LA FACULTAD DE INGENIERÍA

AUTOR: MARIO IVÁN LUJÁN BULLÓN / MEIKHOLL LOPEZ LOPEZ

AÑO: 2010

RESUMEN[4]:

Siendo la universidad un establecimiento diseñado y abocado ha actividades educacionales. Esta es una etapa optativa, pero la de mayor responsabilidad, ya que se encarga de formar a los futuros profesionales del país; por ello es

[4] file:///C:/Users/Downloads/lujan_m.pdf

deber de la universidad velar por la seguridad integral de la comunidad universitaria, el cuidado de su ambiente y la correcta enseñanza. En la actualidad la Universidad Ricardo Palma no cuenta con un Sistema de Gestión en Seguridad y Salud Ocupacional, ni en temas relacionados al medio ambiental que puedan ser aplicados a su campus universitario. Por consiguiente la Universidad Ricardo Palma no es ajena a ello por lo que en el presente trabajo se Elaborará un Modelo de Sistema de Gestión en Seguridad, Salud Ocupacional y Ambiental que pueda ser aplicado en la Facultad de Ingeniería de la Universidad Ricardo Palma. Si bien la URP cuenta con 8 Facultades se decidió elaborar el modelo para la facultad de ingeniería por los siguientes motivos:

- Es la Facultad Ingeniería que reúne la mayor cantidad de estudiantes y cuenta con 2 pabellones. - .Cuenta con Laboratorios de química en la cual emplea como parte experimental y de investigación elementos, sustancias y materiales peligrosos. - Cuenta con laboratorios CIM (Manufactura integrada por Computadora), de cómputo, hidráulica la cual emplea equipos de alta tecnología. Al final del presente estudio la Universidad y la Facultad de Ingeniería tendrían un modelo de Implementación de Gestión para ser aplicado al resto de la universidad que le permita brindar una mayor seguridad y calidad contribuyendo de esta manera al éxito y cuidado de la comunidad universitaria y el ambiente.

TITULO: SISTEMA DE INFORMACIÓN GEOGRÁFICA PARA MEJORAR LA GESTIÓN TÉCNICA DE AGUA POTABLE EN LA EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO EMAPA-HUANCAVELICA

AUTOR: CABALLERO NUÑEZ, José Luis

AÑO: 2017

RESUMEN[5]:

La tesis titulada “Sistema de Información Geográfica Para Mejorar la Gestión Técnica de Agua Potable en la Empresa Municipal de Agua Potable y Alcantarillado EMAPA Huancavelica” tiene como finalidad la gestión técnica eficaz del agua potable, lo cual exige el manejo de una cantidad importante de información. La tesis aborda la problemática actual de la gestión de las redes de agua urbanas mediante la conjunción de las nuevas tecnologías de tratamiento de la información con técnicas innovadoras para la construcción de modelos de las redes de distribución, con el propósito último de facilitar su diagnóstico y extender su uso en la toma de decisiones que redunden en la consecución de los objetivos marcados. La metodología empleada es la modelación de la red de agua a través de sistemas de información geográfica SIG que permita analizar datos y elaborar desde consultas sencillas hasta complejos modelos, llevados a cabo tanto sobre la componente espacial como sobre la componente temática de los datos permitiendo la generación de

5 http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/3362/Caballero%20Nu%C3%B1ez.pdf?sequence=1&isAllowed=y

resultados tales como mapas, informes y gráficos. En donde la naturaleza de esta información se presenta como información física de los elementos de la red, e información espacial sobre la ubicación de estos. Por lo general, esta información era registrada en diversos formatos; la información sobre elementos de la red quedaba guardadas en planos de obra o bases de datos de inventario mientras que la información espacial se encontraba dispersa en distintos planos topográficos donde aparece la ubicación de las tuberías y los trazos de las conducciones de distribución varias veces sin ser actualizadas ya que la conexión entre estos sistemas de información se daba en raras ocasiones o en algunos caos no se daba, por lo que se vio la necesidad de registrar toda esta información en una base de datos centralizada.

Se ha realizado un trabajo que facilitará la toma de decisiones relativas a la gestión técnica en el manejo de una red de agua potable, basando estas decisiones en los resultados proporcionados por un modelo obtenido a partir de los datos incluidos en un Sistema de Información Geográfica. Para ello ha sido necesario solventar una serie de aspectos que se han ido desarrollando a lo largo de los distintos capítulos de la Tesis. Se sugiere ampliar la cobertura de aplicación de los sistemas de información geográfica a las demás áreas de la empresa para así poder tener una gestión integral basada en sistemas de información geográfica.

1.2. Bases Teóricas

1.2.1. Seguridad y Gestión[6]

El Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) abarca una disciplina que trata de prevenir las lesiones y las enfermedades causadas por las condiciones de trabajo, además de la protección y promoción de la salud de los empleados.

Tiene el objetivo de mejorar las condiciones laborales y el ambiente en el trabajo, además de la salud en el trabajo, que conlleva la promoción del mantenimiento del bienestar físico, mental y social de los empleados.

1.2.2. Gestión en Seguridad Y Salud en El Trabajo

El Sistema de Gestión de Seguridad y Salud en el Trabajo de la Universidad Mariana fomenta la participación activa de todas las áreas y programas de la empresa, con el fin de mejorar las condiciones de salud y de trabajo y de la población su laboral y estudiantil, mediante acciones coordinadas de promoción de la salud, la prevención y el control de los riesgos, de manera que faciliten el bienestar de la comunidad laboral y la productividad de la Empresa.

La universidad Mariana, implementa el Sistema de Gestión de Seguridad y Saluden el Trabajo, mediante la planeación, organización, ejecución y evaluación de la procesos y acciones sobre las Condiciones de Salud (medicina preventiva y del trabajo) y de Trabajo (Higiene y Seguridad

[6] https://www.isotools.org/2016/09/06/consiste-sistema-gestion-la-seguridad-salud-trabajo-sg-sst/

Industrial), tendientes a mejorar la salud individual y colectiva de los trabajadores, garantizando el bienestar, la salud de los trabajadores y la productividad de la Empresa[7].

1.2.3. Objetivos Del Sistema De Gestión En Seguridad Y Salud En El Trabajo[8]

Objetivo General:

Implementar, ejecutar, controlar, evaluar y mejorar el Sistema de gestión en Seguridad y Salud en el Trabajo de la Universidad Mariana con el propósito de promover condiciones seguras de trabajo y bienestar laboral a todos los trabajadores; previniendo accidentes de trabajo y enfermedades laborales manteniendo así la calidad de vida de las personas que laboran en esta empresa.

Objetivos Específicos:

- Dar cumplimiento a la legislación vigente en Seguridad y Salud en el trabajo en Colombia.
- Crear el Sistema de gestión en seguridad y salud en el trabajo específico a la actividad económica de la empresa y a las condiciones propias de ella.
- Identificar, evaluar, valorar e intervenir los factores de riesgo a la salud y seguridad e intervenirlos a través de controles desde su causalidad

[7] http://www.umariana.edu.co/dependencias/gestion-talento-humano/index.php/sistema-de-gestion-sst
[8] http://www.umariana.edu.co/dependencias/gestion-talento-humano/index.php/sistema-de-gestion-sst

asociada a la actividad laboral de los trabajadores de la Universidad Mariana.

- Establecer el diagnóstico de seguridad y salud en el trabajo a partir del perfil de condiciones de trabajo y de salud, con el objeto de aplicar los controles preventivos y mecanismos de protección frente al riesgo profesional.
- Establecer acciones dirigidas al ambiente laboral y al trabajador para prevenir los daños a la salud, provenientes de los factores de riesgo presentes en su ámbito laboral.
- Mejorar las condiciones de trabajo y de salud de los trabajadores y controlar las pérdidas en la organización.
- Implementar programas de Vigilancia Epidemiológica orientados a las enfermedades laborales, accidentes de trabajo y por factor de riesgo presente en los centros de trabajo de la Universidad Mariana.
- Fomentar los Estilos de Vida Sana y Trabajo Saludable.
- Asegurar la calidad de las actividades de higiene, seguridad, ergonomía y medicina del trabajo desarrolladas con el propósito de garantizar el control de las condiciones de riesgo causantes de lesiones profesionales.
- Prevenir accidentes de trabajo y enfermedades laborales para preservar el bienestar de los trabajadores y por ende la productividad y eficiencia de la empresa.

- Ubicar y mantener al trabajador según sus aptitudes físicas y psicológicas, en ocupaciones que pueda desempeñar eficientemente sin poner en peligro su salud o la de sus compañeros.
- Brindar todos los recursos y las condiciones específicas para el mejoramiento del Sistema de gestión de seguridad y salud en el trabajo.

1.2.4. Alcance[9]

El Sistema de Gestión de la Seguridad y Salud en el Trabajo de la Universidad Mariana se implementa desde un proceso de programación a partir de la identificación de los peligros, la evaluación de los riesgos, diagnóstico de las condiciones de salud de los trabajadores continuando con la designación de prioridades y objetivos concretos, planeando de acción y ejecutándolas, dando cobertura a todos sus trabajadores en los diferentes centros de trabajo a nivel nacional y regional independiente del tipo de vinculación laboral, logrando la divulgación de los procedimientos del SG-SST a través de la página de Seguridad y Salud en el Trabajo, asegurando el seguimiento y medición del sistema adaptándolo en un proceso de mejora continua.

1.2.5. Servicios que Presta la Seguridad[10]

Para hacer frente a las amenazas a la seguridad del sistema se definen una serie de servicios para proteger los sistemas de procesos de datos y

[9] http://www.umariana.edu.co/dependencias/gestion-talento-humano/index.php/sistema-de-gestion-sst
[10] http://catarina.udlap.mx/u_dl_a/tales/documentos/msp/murillo_c_sr/capitulo1.pdf

de transferencias de información de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

a. **Confidencialidad:** Requiere que la información sea accesible únicamente por las personas y/o áreas autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a solo porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado. La confidencialidad de flujo de tráfico protege la identidad del origen y destino del mensaje, por ejemplo enviando los datos confidenciales a muchos destinos, además del verdadero, así como el volumen y el momento de tráfico intercambiado.

b. **Autenticación:** Requiere una identificación correcta del origen de la información, asegurando que la entidad no es falsa. Se distinguen dos tipos de entidad, que asegura la identidad de las entidades participantes en la comunicación, (huellas dactilares, identificación de iris, etc), tarjetas de banda magnética, contraseñas o procedimientos similares, y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo mas extendido.

c. **Integridad:** Requiere que la información solo pueda ser modificada por las personas autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La

integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera.

d. **No repudio:** Ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizo cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier conflicto. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo mas empleado para este fin.

e. **Control de acceso:** Requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc) sea controlado y limitado por el sistema destino, mediante el uso de contraseña o llaves hardware, por ejemplo protegiéndose frente a usos no autorizados o manipulaciones.

1.3. Marco Conceptual

1.3.1. Seguridad Informática[11]

La seguridad informática es un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema**.**

[11] https://www.significados.com/seguridad-informatica/

La seguridad informática se caracteriza por la protección de datos y de comunicaciones en una red asegurando, en la medida de lo posible, los tres principios básicos:

La integridad de los datos: la modificación de cualquier tipo de información debe ser conocido y autorizado por el autor o entidad.

La disponibilidad del sistema: la operación continua para mantener la productividad y la credibilidad de la empresa.

La confidencialidad: la divulgación de datos debe ser autorizada y los datos protegidos contra ataques que violen este principio.

La seguridad informática es una disciplina o rama de la Tecnología de la información, que estudia e implementa las amenazas y vulnerabilidades de los sistemas informáticos especialmente en la red como, por ejemplo, virus, gusanos, caballos de troya, ciber-ataques, ataques de invasión, robo de identidad, robo de datos, adivinación de contraseñas, intercepción de comunicaciones electrónicas, entre otros.

Tipos de seguridad informática

La seguridad Informática suele dividirse en tres clases:

Seguridad de *hardware*

La seguridad de *hardware* implica tanto la protección física como el control del tráfico de una red y el escáner constante de un sistema. Algunos ejemplos de seguridad informática de *hardware* son los cortafuegos de hardware, servidores proxys y claves criptográficas para cifrar, descifrar y

autentificar sistemas, copias de seguridad, bancos de baterías para los cortes de electricidad, etc.

Seguridad de *software*

La seguridad de *software* se dedica a bloquear e impedir ataques maliciosos de *hackers*, por ejemplo. La seguridad de *software* es parte del proceso de la implementación de un programa, trabajo de ingenieros informáticos, para prevenir modificaciones no autorizadas que cause el mal funcionamiento o violación de la propiedad intelectual del programa en sí.

Seguridad de red

La seguridad informática en la red es aplicada a través del *hardware* y el *software* del sistema. La seguridad en la red protege la facilidad de uso, la fiabilidad, la integridad, y la seguridad de la red y de los datos. Algunos componentes que ayudan en este aspecto son: los antivirus, *antispyware*, cortafuegos que cortan el acceso no autorizado, redes privadas virtuales (VPN) y sistema de prevención de intrusos (IPS).

1.3.2. Mecanismos de Seguridad[12]

Los aspectos de seguridad comúnmente aceptados son los siguientes:

- Identificación y autenticación
- Autorización
- Auditoría
- Confidencialidad
- Integridad de datos

[12] https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009730_.htm

Los *mecanismos de seguridad* son herramientas técnicas y métodos técnicos que se utilizan para implementar los servicios de seguridad. Un mecanismo puede funcionar por sí solo, o con otros, para proporcionar un servicio determinado. Los siguientes son ejemplos de mecanismos de seguridad comunes:

- Cifrado
- Resúmenes de mensajes y firmas digitales
- Certificados digitales
- Infraestructura de claves públicas (PKI)

Cuando planifique una implementación de WebSphere MQ, considere qué mecanismos de seguridad necesita para implementar estos aspectos de seguridad que son importantes para usted. Para obtener información acerca de lo que ha de tener en cuenta después de que haya leído estos temas, consulte Planificación de los requisitos de seguridad.

Identificación y autenticación[13]

La *identificación* es la capacidad de identificar de forma exclusiva a un usuario de un sistema o una aplicación que se está ejecutando en el sistema. La *autenticación* es la capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser.

- **Autorización**

  La *autorización* protege los recursos importantes de un sistema, ya que limita el acceso solamente a los usuarios autorizados y a sus

[13] https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009730_.htm

aplicaciones. Impide que los recursos se utilicen sin la autorización necesaria.

- **Auditoría**

  La *auditoría* es el proceso de registrar y comprobar sucesos para detectar si ha tenido lugar una actividad no esperada o no autorizada, o si se ha llevado a cabo algún intento para realizar dicha actividad.

- **Confidencialidad**

  El servicio de *confidencialidad* protege la información confidencial para que no pueda divulgarse sin la autorización correspondiente.

- **Integridad de datos**

  El servicio de *integridad de datos* detecta si se han modificado los datos de forma no autorizada.

- **Conceptos de cifrado**

  En esta colección de temas se describen los conceptos de cifrado aplicables a WebSphere MQ.

- **Protocolos de seguridad de cifrado: SSL y TLS**

Los protocolos de cifrado proporcionan conexiones seguras, permitiendo que dos partes se comuniquen con privacidad e integridad de datos. El protocolo TLS (Transport Layer Security) ha evolucionado a partir del protocolo SSL (Secure Sockets Layer). WebSphere MQ da soporte tanto a SSL como a TLS.

1.3.3. Protocolos de Seguridad

Un protocolo de seguridad es un conjunto de intercambios en los que intervienen normalmente dos o tres entidades: La entidad iniciadora del protocolo (entidad a), la entidad receptora (entidad b) y una tercera entidad opcional (entidad c) con la misión de autenticación de los intercambios, distribución de claves públicas y/o claves de sesión. El objetivo principal de un protocolo de seguridad es distribuir una clave de sesión de forma segura entre las entidades a y b con el objetivo de tener un canal seguro de datos entre estas entidades. Una forma de definir los intercambios que comprenden un protocolo de seguridad es utilizar especificaciones formales. En la figura vemos la especificación formal que utilizaremos para representar protocolos de seguridad. En este ejemplo solo intervienen dos entidades a y b:

La especificación formal que utilizaremos para representar protocolos de seguridad se compone de cuatro campos Identificador de inicio de la especificación, Declaración de Constantes, Mensajes implicados en el protocolo de seguridad, Declaración de Relaciones asociadas a mensajes: Identificador de inicio de la especificación: Este elemento determina el comienzo de la especificación formal de un protocolo de seguridad y está formado únicamente por la cadena de caracteres “PROTOCOL SPECIFICATION”. Declaración de Constantes: Este elemento contiene las

cadenas de caracteres que denominaremos identificadores constantes que se utilizarán en la definición del protocolo de seguridad. Es decir este campo comienza con la cadena de caracteres “CONSTANTS” seguida en líneas distintas de los identificadores presentes en la especificación agrupados por tipos. Cada tipo de constantes aparecerá en una línea y separado del siguiente por el carácter “;” y a su vez los identificadores asociados a un tipo concreto aparecerán dentro del tipo separados por comas (“,”). El elemento finaliza con el carácter (“.”) después del último tipo de identificadores.

1.3.4. Sistema de Seguridad

En los siguientes capítulos se estudiarán las distintas funciones que se deben asegurar en un sistema informático.

1. Reconocimiento: cada usuario deberá identificarse al usar el sistema y cada operación del mismo será registrada con esta identificación. En este proceso seque no se produzca un acceso y/o manipulación indebida de los datos o que en su defecto, esta quede registrada.
2. Integridad: un sistema integro es aquel en el que todas las partes que lo constituyen funcionan en forma correcta y en su totalidad.
3. Aislamiento: Los datos utilizados por un usuario deben ser independientes de los de otro física y lógicamente (usando técnicas de ocultación y/o compartimiento).

4. Auditabilidad: procedimiento utilizado en la elaboración de exámenes, demostraciones, verificaciones o comprobaciones del sistema. Estas comprobaciones deben ser periódicas y tales que brinden datos precisos y aporten confianza a la dirección. Deben apuntar a contestar preguntas como:

    - ¿El uso del sistema es adecuado?
    - ¿El sistema se ajusta a las normas internas y externas vigentes?
    - ¿Los datos arrojados por el sistema se ajustan a las expectativas creadas?
    - ¿Todas las transacciones realizadas por el sistema pueden ser registradas adecuadamente?
    - ¿Contienen información referente al entorno: tiempo, lugar, autoridad, recurso, empleado, etc.?

5. Controlabilidad: todos los sistemas y subsistemas deben estar bajo control permanente.
6. Recuperabilidad: en caso de emergencia, debe existir la posibilidad de recuperarlos recursos perdidos o dañados.
7. Administración y Custodia: la vigilancia nos permitirá conocer, en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una realimentación del sistema de seguridad, de forma tal de mantenerlo actualizado contra nuevas amenazas.

1.4. Importancia de la Investigación

Se considera de vital importancia el presente proyecto de tesis por cuanto, la principal función del proyecto de investigación será diseñar un modelo de seguridad informática en las oficinas de la Empresa Municipal de Agua potable y Alcantarillado de Ica, que le permitan poder determinar cuan confiables son los sistemas que utilizan para el manejo de la información; es por ello que se hace importante poder mejorar dichos sistemas de seguridad, ya que la auditoria de sistemas no se realiza con frecuencia dentro de los sistemas con que cuenta la Empresa. Asimismo no cuenta con personal capacitado para realizar una labor de monitoreo en todos los sistemas en las distintas oficinas administrativas.

CAPITULO II: EL PROBLEMA OBJETIVOS E HIPOTESIS

2.1. El Problema de Investigación

2.1.1. Planteamiento del problema

La empresa municipal de agua potable y alcantarillado de Ica, teniendo en cuenta la situación actual de la empresa y los estimados de crecimiento del número de unidades de uso de agua y alcantarillado, se ha propuesto un programa de inversiones quinquenal sobre la base de la información del Plan de seguridad informática para mejorar el grado de confiabilidad de los equipos informáticos.

Según cálculos internacionales, cada trabajador dedica alrededor de media hora diaria para solucionar o solicitar ayuda relacionada a problemas informáticos de todo tipo, que van desde fallas tan simples como un mouse en mal estado hasta situaciones más complejas como fallas computacionales y de sistemas por causa de virus, gusanos u otras amenazas. Son estos últimos contratiempos los que generan un mayor freno en la productividad en las empresas, pues según datos de la compañía de seguridad informática NovaRed, los trabajadores pueden llegar a perder más de 100 horas anuales intentando solucionar este tipo de fallas de seguridad.

Según Hans Erpel, gerente comercial de NovaRed, esta situación genera una pérdida irrecuperable para las empresas, lo que convierte a la seguridad informática en una preocupación clave. “Cada vez los problemas relacionados netamente con ataques en la red van creciendo en cantidad y complejidad, por lo que esta área debe ser primordial en cada una de las

compañías, no sólo para aminorar las horas perdidas en solucionar este tipo de defectos, sino también para disminuir las vulnerabilidades computacionales y mantener la continuidad del

negocio”

Erpel enfatiza que es primordial invertir en seguridad informática y no verla como un costo. “Muchas compañías asumen que no han sido víctimas de algún ataque informático sin tener realmente esa certeza y otras adoptan una actitud de tranquilidad ante el tema, pensando que basta sólo con contar con un sistema de prevención y olvidando que la seguridad cumple un ciclo de vida que requiere un constante trabajo de evaluación, proceso de rediseño, implementación y por último una correcta administración, monitoreo y soporte de los servicios”.

Ante todo lo indicado la empresa Municipal de Agua potable y alcantarillado de Ica plantea las siguientes preguntas: ¿Quién no ha tenido alguna vez un inconveniente con el computador del trabajo? ¿Realizando un servicio de seguridad se mantendrá un control sobre la información de la empresa? ¿Llevar a cabo un control sobre la seguridad informática en la empresa mejorara el control de los equipos de cómputo de la empresa?

2.1.2. Formulación del problema

Problema General

PG: ¿En qué medida el modelo de un sistema de seguridad informática influye en mejorar el manejo de la información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA?

Problemas específicos

PE_1: ¿En qué medida el modelo de un sistema de seguridad informática influye en mejorar el tiempo solicitado en pedir información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA?

PE_2: ¿En qué medida el modelo de un sistema de seguridad informática influye en mejorar el tiempo en crear copia de seguridad de la información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA?

2.1.3. Delimitación del problema

a. Delimitación Espacial

El área de estudio que abarcara el presente proyecto de tesis comprende la Localidad de Ica, en donde se ubica la empresa municipal de agua potable y alcantarillado de Ica sito en la calle castrovirreyna No 487.

b. Delimitación Temporal

El desarrollo de la tesis en esta primera fase tiene un horizonte temporal durante el año 2017 comprendido de la siguiente manera:

Primera Etapa: Corresponde a la parte de la elaboración del Plan de Tesis desde el capítulo I, constituido por el planteamiento metodológico y el capítulo II, conformado por la elaboración del marco teórico. Y está delimitada entre el 25 de Marzo al 20 de Julio del 2017.

Segunda Etapa: Comprende la parte de la Investigación de Tesis, Análisis del sistema de inteligencia de negocios, el análisis e interpretación de resultados, contrastación de la hipótesis, las conclusiones y recomendaciones, y la presentación del informe final en Diciembre del 2017.

c. Delimitación Social

En el desarrollo de la tesis están involucrados diversos roles sociales, los que a continuación se van a nombrar:

- El investigador
- El asesor
- Personal del área de computo
- Trabajadores administrativos

2.2. Objetivos de la Investigación

2.2.1. Objetivo General

OG: Determinar como el modelo de un sistema de seguridad informática mejora la seguridad de la información en la empresa municipal de agua potable y alcantarillado de Ica.

2.2.2. Objetivos Específicos

OE1: Determinar como el modelo de un sistema de seguridad informática mejora el tiempo solicitado en solicitar información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA.

OE2: Determinar como el modelo de un sistema de seguridad informática mejora el tiempo en crear copia de seguridad de la información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA

2.3. Hipótesis de la Investigación

2.3.1. Hipotesis General

HG: El diseño de un modelo de seguridad Informática influye en mejorar la información en la empresa municipal de agua potable y alcantarillado de Ica – EMAPICA.

2.3.2. Hipotesis Especifica

HE1: El diseño de un modelo de seguridad Informática influye en mejorar el tiempo solicitado para la información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA.

HE2: El diseño de un modelo de seguridad Informática influye en mejorar el tiempo en crear copia de seguridad de la información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA

CAPITULO III: METODOLOGIA DE INVESTIGACION

3.1. Tipo de investigación

El presente proyecto de tesis fue de tipo Aplicada y de naturaleza practica

3.2. Nivel de investigación

La investigación fue de nivel práctico

3.3. Variables e Indicadores

Variable Independiente:

X: Sistema de Seguridad Informática

Variable Dependiente:

Y: Aplicación del mejoramiento de la información

Y_1: Tiempo solicitado para la información

Y_2: Tiempo en crear copia de seguridad de la información.

Tabla 01: optimización de los indicadores

Indicador	U. Medida	Índice	U. Observación
Y_1: Tiempo solicitado para la información .	Min.	[10..20]	Guía de Observación
Y_2: Tiempo en crear copia de seguridad de la información	Min.	[15 .. 30]	Guía de Observación

Tabla N° 032: 0peracionalización de Indicadores

Indicador	Conceptualización
Y_1= Tiempo solicitado para la información	Es el tiempo que se solicita para mejorar la seguridad.
Y_2= Tiempo en crear copia de seguridad de la información	Tiempo requerido para crear copias de seguridad de la información.

3.4. Población y muestra

3.4.1. Población.

Para el presente proyecto de tesis se utilizó una población de 50 personas entre personal administrativo y el personal del centro de cómputo N= 50.

3.4.2. Muestra.

N=	Población	50	$n' = \frac{S^2}{V^2}$	al 95% de confianza
se=	error estandar	0.05		
p=	% estimado	0.5		
				S^2 = Varianza de la población
S2	Varianza Población	0.25	S^2= p(1-p)	V^2= varianza de la muestra
V2	Varianza Muestra	0.0025	V^2= se^2	P=porcentaje estimado de la muestra

$$n' = \frac{S^2}{V^2}$$

n'= 0.25 / 0.0025 = 100

$$n = \frac{n'}{1 + \frac{n'}{N}}$$

n= 100 / 3 = 33.33 → 33.00

n=33

Diseño del método de investigación

La investigación se desarrolló bajo un diseño experimental. El diseño experimental es cuando a través de un experimento se busca llegar a la causa de un fenómeno. Tiene como esencia la de someter el objeto de estudio a la influencia de ciertas variables en condiciones controladas y conocidas por el investigador (Tamayo, 2004).

3.5 Técnicas de recolección de información

Las técnicas de recolección de información del presente trabajo de tesis fueron los siguientes:

a. Entrevistas
b. Observación
c. Análisis

3.6. Instrumentos de recolección de información

- Guía de observación: con este instrumento Guía de observación se anotaron los datos requeridos para los indicadores.
- Guía de entrevista: con este instrumento se pudo registrar la información de áreas referentes a los indicadores.
- Fichas documentales: con este instrumento se pudo recoger toda la información que corresponde a las fuentes de datos.

3.7. Técnicas de análisis e interpretación de datos y resultados

Las técnicas de análisis e interpretación de los datos, se ejecutaron con el software estadístico Minitab, y las pruebas que se realizan son: a) pruebas estadísticas descriptivas y b) pruebas de inferencia para contrastar la hipótesis.

Para la prueba estadística descriptiva, se analizan las medidas de tendencia central y las pruebas de variabilidad de los datos, los mismos que serán graficados para mejorar su análisis.

En la prueba de inferencia se realiza la prueba para datos cuantitativos como t (siempre que nuestra muestra sea menor o igual a 30 unidades de análisis); y la prueba z(siempre que la muestra sea mayor a 30 unidades de análisis), el resultado se representa en la curva de Gauss, para ver la aceptación o rechazo de la hipótesis nula.

CAPITULO IV: MODELO PARA LA SEGURIDAD INFORMATICA

4.1. Seguridad Física

Es muy importante ser consciente que por más que la empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc.; la seguridad de la misma será nula si no se ha previsto como combatir los ataques.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Así, la **Seguridad Física** consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

4.1.1. Tipos de Desastres

No será la primera vez que se mencione en este trabajo, que cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física de la empresa son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara. A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

A continuación se analizan los peligros más importantes que se corren en un el centro de procesamiento de la empresa Emapica; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para

la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos

4.1.2. Incendios

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Desgraciadamente los sistemas anti fuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputos.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

1. El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
2. El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
3. Las paredes deben hacerse de materiales incombustibles y

extenderse desde el suelo al techo.

4. Debe construirse un “falso piso” instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
5. No debe estar permitido fumar en el área de proceso.
6. Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.
7. El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

4.1.3. Seguridad del Equipamiento

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

Figura 01 Procesos de Seguridad

4.1.4. Condiciones Climatológicas

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

Ica, lugar donde se encuentra la Empresa Municipal de Agua Potable y Alcantarillado de Ica Emapica, es una zona altamente sísmica ya que frecuentemente ocurren sismos. Algunos sismos menores hasta los de gran intensidad como los terremotos.

Otro fenómeno climatológico que se aprecia en la ciudad de Ica son los Paracas, son fuertes vientos que ocasionan levantes de polvo y arena a su paso, reduciendo la visibilidad.

También tenemos la ocurrencia cada cierto tiempo en la región de Ica, del fenómeno del niño que tiene como consecuencia la ocurrencia de fuertes lluvias, aumento excesivo del caudal de los ríos.

La frecuencia y severidad de su ocurrencia de los fenómenos climatológicos, deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, sismos, lluvias u otros fenómenos climatológicos permiten que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

Terremotos

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros.

El año 2007 un terremoto sacudió la región de Ica, causando daños y destrucción en las viviendas, construcciones como carreteras, puentes registrándose también gran cantidad de personas heridas y pérdidas humanas.

Para estos casos, se recomienda tener los equipos informáticos, dispositivos en ambientes que sean considerados seguros ante la ocurrencia de un sismo.

4.1.5. Instalación Eléctrica

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Picos y Ruidos Electromagnéticos

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

Cableado

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el

tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

1. Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.
2. Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
3. Daños en el cable: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos.

En la Empresa Emapica, se observó un poco de cables en desorden, en el suelo. Cables de corrientes de los dispositivos, cables de red, que pueden ocasionar que las personas se puedan caer y también el riesgo que

supone ya que transmiten energía eléctrica. Se recomendó, ordenar los cables con canaletas, tubos corrugados, pasacables de suelo, poner zócalos pasacables.

4.1.6. Sistema De Aire Acondicionado

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

Figura 02: Emisiones Electromagnéticas

Desde hace tiempo se sospecha que las emisiones, de muy baja frecuencia que generan algunos periféricos, son dañinas para el ser humano.

Según recomendaciones científicas estas emisiones podrían reducirse mediante filtros adecuados al rango de las radio frecuencias, siendo estas totalmente seguras para las personas.

Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar su envejecimiento.

4.2. Acciones Hostiles

4.2.1 Robo

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro

4.2.2 Fraude

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

Figura 03 : Fraude Informático

4.2.3 Sabotaje

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos. Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

4.3 Control De Accesos

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

4.3.1 Utilización De Guardias

Control De Personas

El Servicio de Vigilancia es el encargado del control de acceso de todas las personas al edificio. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

A cualquier personal ajeno a la planta se le solicitará completar un formulario de datos personales, los motivos de la visita, hora de ingreso y de egreso, etc.

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa.

En este caso la persona se identifica por **algo que posee**, por ejemplo una tarjeta de identificación. Cada una de ellas tiene un PIN (Personal

Identification Number) único, siendo este el que se almacena en una base de datos para su posterior seguimiento, si fuera necesario.

Su mayor desventaja es que estas tarjetas pueden ser copiadas, robadas, etc., permitiendo ingresar a cualquier persona que la posea.

Estas credenciales se pueden clasificar de la siguiente manera:

- Normal o definitiva: para el personal permanente de planta.
- Temporaria: para personal recién ingresado.
- Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.
- Visitas.

Las personas también pueden acceder mediante **algo que saben** (por ejemplo un número de identificación o una password) que se solicitará a su ingreso. Al igual que el caso de las tarjetas de identificación los datos ingresados se contrastarán contra una base donde se almacena los datos de las personas autorizadas. Este sistema tiene la desventaja que generalmente se eligen identificaciones sencillas, bien se olvidan dichas identificaciones o incluso las bases de datos pueden verse alteradas o robadas por personas no autorizadas.

4.3.2. Protección Electrónica

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los

encargados de hacerles saber al personal de una situación de emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

Barreras Infrarrojas Y De Micro–Ondas

Transmiten y reciben haces de luces infrarrojas y de micro–ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuestas por un transmisor y un receptor de igual tamaño y apariencia externa. Cuando el haz es interrumpido, se activa el sistema de alarma, y luego vuelve al estado de alerta. Estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc.

Las invisibles barreras fotoeléctricas pueden llegar a cubrir áreas de hasta 150 metros de longitud (distancias exteriores). Pueden reflejar sus rayos por medio de espejos infrarrojos con el fin de cubrir con una misma barrera diferentes sectores.

Las micro–ondas son ondas de radio de frecuencia muy elevada. Esto permite que el sensor opere con señales de muy bajo nivel sin ser afectado por otras emisiones de radio, ya que están muy alejadas en frecuencia.

Debido a que estos detectores no utilizan aire como medio de propagación, poseen la ventaja de no ser afectados por turbulencias de aire o sonidos muy fuertes.

Otra ventaja importante es la capacidad de atravesar ciertos materiales como son el vidrio, lana de vidrio, plástico, tabiques de madera, revoques sobre madera, mampostería y hormigón.

Detector Ultrasónico

Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generará una perturbación en dicho campo que accionará la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas. La cobertura de este sistema puede llegar a un máximo de 40 metros cuadrados.

Circuitos Cerrados De Televisión

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizada como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

Todos los elementos anteriormente descriptos poseen un control contra sabotaje, de manera que si en algún momento se corta la alimentación o

se produce la rotura de alguno de sus componentes, se enviará una señal a la central de alarma para que ésta accione los elementos de señalización correspondientes.

Edificios Inteligentes

La infraestructura inmobiliaria no podía quedarse rezagada en lo que se refiere a avances tecnológicos. El Edificio Inteligente (surgido hace unos 10 años) se define como una estructura que facilita a usuarios y administradores, herramientas y servicios integrados a la administración y comunicación. Este concepto propone la integración de todos los sistemas existentes dentro del edificio, tales como teléfonos, comunicaciones por computadora, seguridad, control de todos los subsistemas del edificio (gas, calefacción, ventilación y aire acondicionado, etc.) y todas las formas de administración de energía.

Figura 04: Edificios Inteligentes

4.4 Seguridad Lógica

Luego de ver como nuestro sistema puede verse afectado por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la **información**, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la **Seguridad Lógica** consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.

- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

4.4.1. Controles De Acceso

Estos controles 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.

Asimismo, 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. Al respecto, 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:

4.4.2. Identificación Y Autentificación

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.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
2. Algo que la persona **posee:** por ejemplo una tarjeta magnética.
3. Algo que el individuo **es** y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single log–in" o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos,

basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

1. Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.
2. Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
3. Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.
4. Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de

acceso.

5. Detección de actividades no autorizadas. Además de realizar auditorías o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.
6. Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
7. Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

Imagen 01: Formulario de Acceso

4.4.3. Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

4.4.4. Transacciones

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

4.4.5. Limitaciones 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. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

4.4.6. Ubicación Y Horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

Figura 05: Ubicación y horario

4.4.7. Control De Acceso Interno

Palabras Claves (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 clave 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.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

- **Sincronización de passwords**: consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar una sola password para todos los sitios a los que tengan acceso, y que si se los fuerza a elegir diferentes passwords tienden aguardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.
- **Caducidad y control:** este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen.

Encriptación

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

Este tema será abordado con profundidad en el Capítulo sobre Protección del presente.

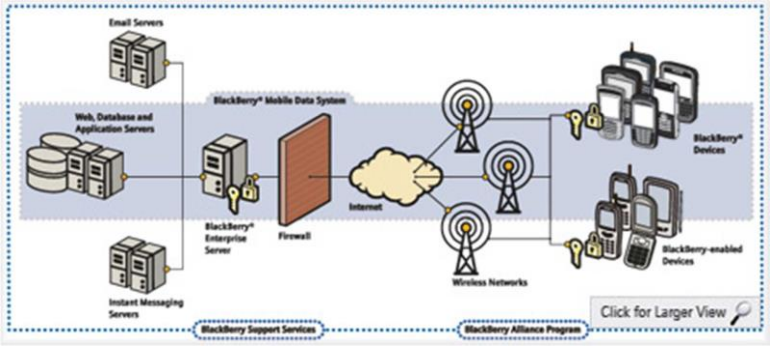


Figura 06: Encriptación

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.

Límites Sobre La Interfase De Usuario

Esto 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. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

Etiquetas De Seguridad

Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

4.4.8. Control De Acceso Externo

Dispositivos De Control De Puertos

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

Firewalls 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 con posterioridad.

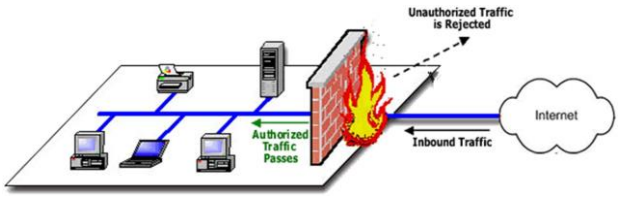


Figura 07: Puertas de Seguridad

4.5. Niveles De Seguridad Informática

El estándar de niveles de seguridad más utilizado internacionalmente es el TCSEC Orange Book, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.

Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.

4.5.1. Nivel D

Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna

especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS–DOS y System 7.0 de Macintosh.

4.5.2. Nivel C1: Protección Discrecional

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este “súper usuario”; quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- Acceso de control discrecional: distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de

ellos.

- Identificación y Autentificación: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

4.5.3. Nivel C2: Protección De Acceso Controlado

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringirá aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

4.5.4. Nivel B1: Seguridad Etiquetada

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

4.5.5. Nivel B2: Protección Estructurada

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la

primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

4.5.6. Nivel B3: Dominios De Seguridad

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.

Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

4.5.7. Nivel A: Protección Verificada

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Figura 08: Protección verificada

CAPITULO V: ANALISIS E INTERPRETACION DE RESULTADO

5.1. Para Los Datos De La Pre Prueba

PARA EL INDICADOR 1: Tiempo solicitado para la información

Para esta investigación el tiempo solicitado para la información, se mide de acuerdo al índice así mismo la magnitud del error sea tolerable y el riesgo admisible, se requiere un tamaño de muestra en la que se asegure un 95% de probabilidad de que el error no sea superior al 5%.

Considerando que el tamaño de muestra en pre-prueba es de 33 observaciones referidas al tiempo solicitado para la información, en la tabla 01 se muestran los datos aleatorios y en la tabla 02 los datos derivados del análisis de los datos de la tabla 01. Estos datos de pre-prueba ayudaran para contrastar los tiempos de control de la información.

Tabla 03: Datos aleatorios del indicador 1

U_analisis	TSI_pre	TSI_Pos
1	13	13
2	27	8
3	19	8
4	14	11
5	22	12
6	29	12
7	23	9
8	27	9
9	18	10
10	13	8
11	19	9
12	11	12
13	25	8
14	26	13
15	18	12
16	23	15
17	11	12
18	28	8
19	20	12

20	14	9
21	15	11
22	19	9
23	14	9
24	26	10
25	25	11
26	20	13
27	27	9
28	12	11
29	10	11
30	22	10
31	25	15
32	22	8
33	23	8

Tabla 04: Tabla del análisis de los datos del indicador 1

U_analisis	TSI_pre	TSI_Pos
1	27.46	12.84
2	13.67	11.57
3	28.26	9.60
4	19.06	9.91
5	17.18	12.93
6	24.68	13.08
7	16.19	10.52
8	21.92	11.14
9	20.32	11.71
10	23.75	11.78
11	21.54	10.88
12	20.27	9.30
13	23.49	11.55
14	29.39	14.78
15	23.94	14.87
16	19.74	13.30
17	20.92	13.28
18	21.65	13.71
19	15.21	12.18
20	10.29	13.40
21	19.83	11.99
22	16.56	11.06
23	13.77	10.86
24	6.15	10.54
25	17.50	13.28
26	10.66	10.23

27	30.52	14.28
28	23.32	13.18
29	24.05	8.91
30	15.21	12.72
31	18.14	10.68
32	17.44	9.38
33	21.61	12.60

PARA EL INDICADOR 2: Tiempo en crear copia de seguridad de la información.

Para esta investigación el tiempo en crear copia de seguridad de la información, se mide de acuerdo al índice así mismo la magnitud del error sea tolerable y el riesgo admisible, se requiere un tamaño de muestra en la que se asegure un 95% de probabilidad de que el error no sea superior al 5%.

Considerando que el tamaño de muestra en pre-prueba es de 33 observaciones referidas al tiempo solicitado para la información, en la tabla 01 se muestran los datos aleatorios y en la tabla 02 los datos derivados del análisis de los datos de la tabla 01. Estos datos de pre-prueba ayudaran para contrastar los tiempos de control de la información.

Tabla 05: Datos aleatorios del indicador 2.

U_analisis	TCCS_Pre	TCCS_Pos
1	27	14
2	15	13
3	21	16
4	26	20
5	23	18
6	17	18
7	15	19
8	19	13

9	20	19
10	17	15
11	15	18
12	26	11
13	18	14
14	20	11
15	24	15
16	21	18
17	26	14
18	23	17
19	24	20
20	29	13
21	25	19
22	20	10
23	30	19
24	29	19
25	17	16
26	30	17
27	20	18
28	15	15
29	19	15
30	15	15
31	17	12
32	18	20
33	28	17

Tabla 06: Tabla del análisis de los datos del indicador 2

U_analisis	TCCS_Pre	TCCS_Pos
1	28.82	11.99
2	23.39	18.24
3	16.68	14.34
4	24.63	11.82
5	20.31	20.75
6	21.06	11.41
7	18.44	13.98
8	18.27	13.57
9	21.01	12.02
10	23.42	12.75
11	18.41	10.01
12	21.72	8.16
13	27.58	15.68
14	22.51	15.18
15	21.66	11.99

16	26.77	19.13
17	11.76	16.45
18	26.91	15.24
19	16.08	11.08
20	15.05	4.31
21	21.16	18.10
22	23.23	13.58
23	27.84	12.77
24	22.99	14.37
25	21.40	12.16
26	23.91	13.16
27	17.61	14.96
28	31.75	9.74
29	22.70	6.12
30	14.41	12.11
31	27.19	15.82
32	13.93	20.25
33	24.21	21.05

5.2. Contrastación de las hipótesis

5.2.1. Contrastación de la hipótesis general

Ha: El diseño de un modelo de seguridad Informática influye en mejorar la información en la empresa municipal de agua potable y alcantarillado de Ica – EMAPICA.

Ho: El diseño de un modelo de seguridad Informática No influye en mejorar la información en la empresa municipal de agua potable y alcantarillado de Ica – EMAPICA.

5.2.2. Contrastación de las hipótesis específicas

A. Hipótesis Específica 1:

Ha1: El diseño de un modelo de seguridad Informática influye en mejorar Tiempo solicitado para la información en la empresa municipal de agua potable y alcantarillado de Ica – EMAPICA.

Ho1: El diseño de un modelo de seguridad Informática **No** influye en mejorar Tiempo solicitado para la información en la empresa municipal de agua potable y alcantarillado de Ica – EMAPICA.

Aplicamos la Prueba de Wilcoxon, en el programa estadístico SPSS, arrojándonos los siguientes resultados:

Prueba de rangos con signo de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
TSI_pos - TSI_pre	Rangos negativos	31[a]	17,61	546,00
	Rangos positivos	2[b]	7,50	15,00
	Empates	0[c]		
	Total	33		

a. TSI_pos < TSI_pre

b. TSI_pos > TSI_pre

c. TSI_pos = TSI_pre

Estadísticos de prueba[a]

	TSI_pos - TSI_pre
Z	-4,744[b]
Sig. asintótica(bilateral)	0,000002

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

En este caso como el nivel de significancia de 0,000002 es menor que 0.05, entonces se rechaza la hipótesis nula y se acepta la hipótesis alternativa **Ha1,** por lo tanto el diseño de un modelo de seguridad Informática influye en mejorar Tiempo solicitado para la información en la empresa municipal de agua potable y alcantarillado de Ica **– EMAPICA.**

B. Hipótesis Específica 2:

Ha2: El diseño de un modelo de seguridad Informática influye en mejorar Tiempo en crear copia de seguridad de la información en la empresa municipal de agua potable y alcantarillado de Ica – EMAPICA.

Ho2: El diseño de un modelo de seguridad Informática **No** influye en mejorar Tiempo en crear copia de seguridad de la información en la empresa municipal de agua potable y alcantarillado de Ica – EMAPICA.

Aplicamos la Prueba de Wilcoxon, en el programa estadístico SPSS, y nos muestra los siguientes resultados:

Prueba de rangos con signo de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
TCCS_post - TCCS_pre	Rangos negativos	30[a]	18,00	540,00
	Rangos positivos	3[b]	7,00	21,00
	Empates	0[c]		
	Total	33		

a. TCCS_post < TCCS_pre

b. TCCS_post > TCCS_pre

c. TCCS_post = TCCS_pre

Estadísticos de prueba[a]

	TCCS_post - TCCS_pre
Z	-4,637[b]
Sig. asintótica(bilateral)	0,000004

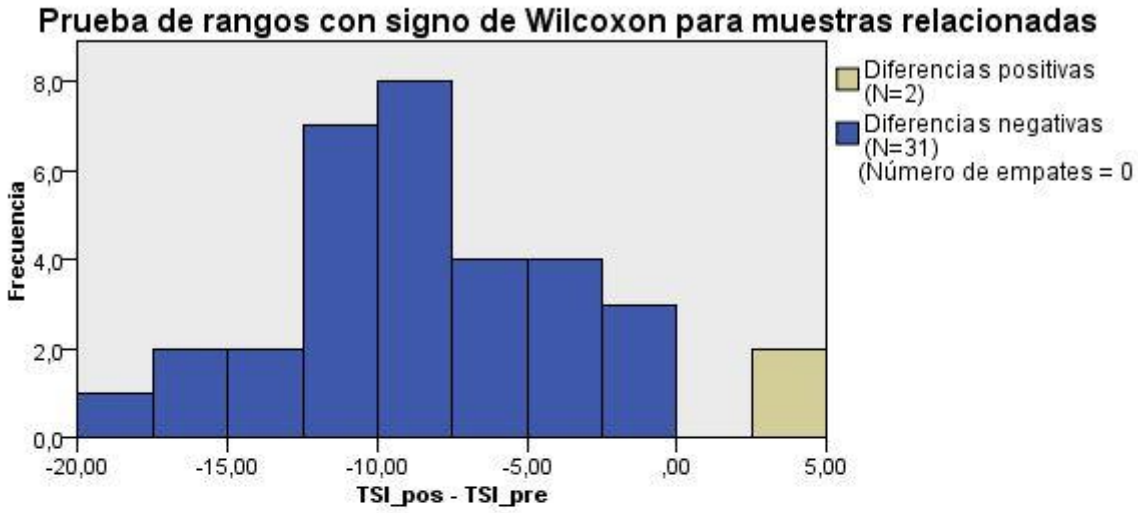
a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

En este caso se observa que el nivel de significancia de 0,000004 es menor que 0.05, entonces se rechaza la hipótesis nula y se acepta la hipótesis alternativa **Ha2,** por lo tanto el diseño de un modelo de seguridad Informática influye en mejorar Tiempo en crear copia de seguridad de la información en la empresa municipal de agua potable y alcantarillado de Ica – EMAPICA.

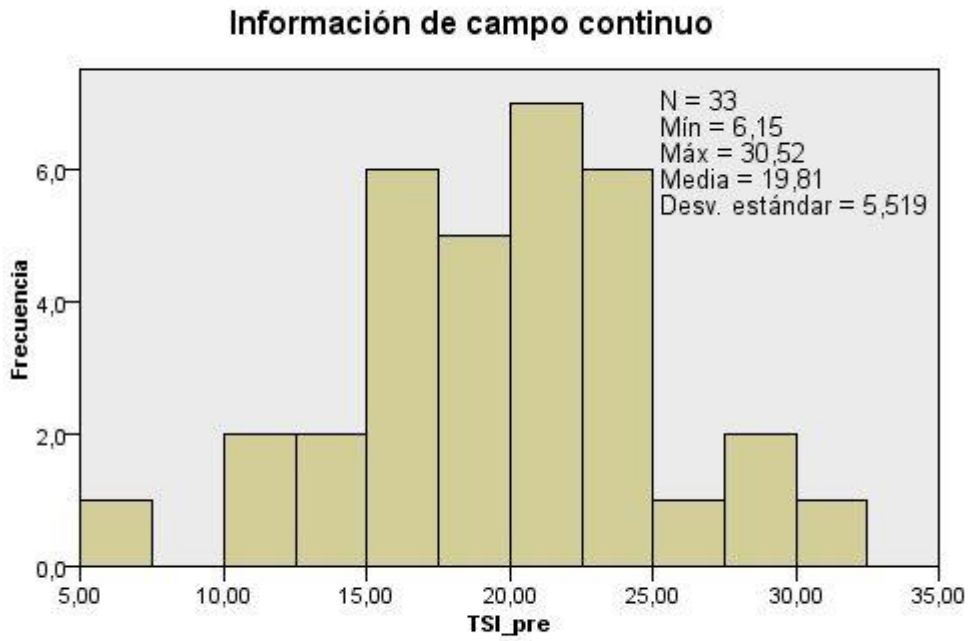
5.3. Presentación, interpretación y discusión de resultados

Indicador 1: Tiempo solicitado para la información



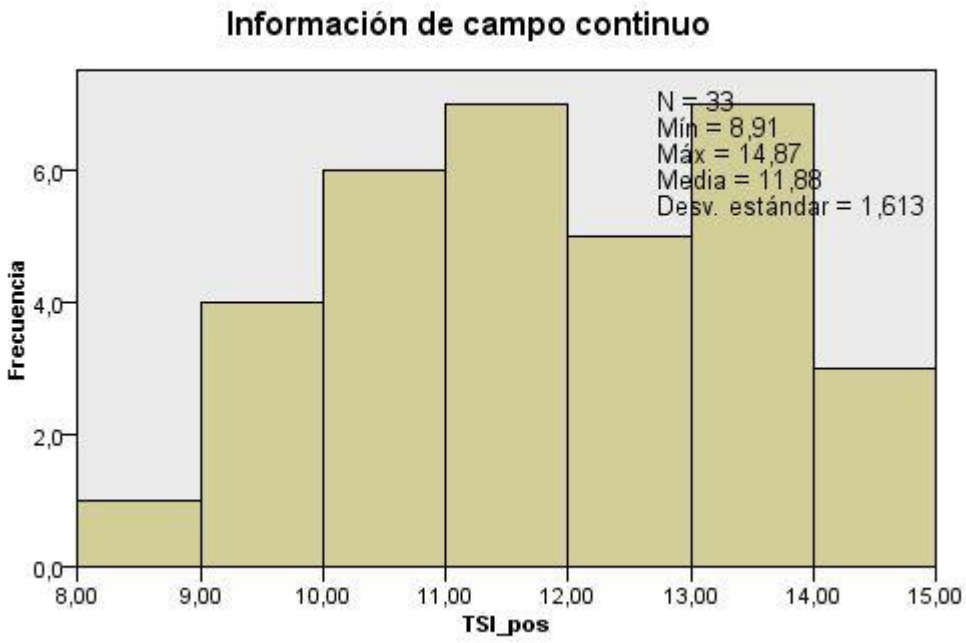
N total	33
Estadístico de contraste	15,000
Error estándar	55,967
Estadístico de contraste estandarizado	-4,744
Sig. asintótica (prueba bilateral)	,000

Información de Campo Continuo TSI-pre



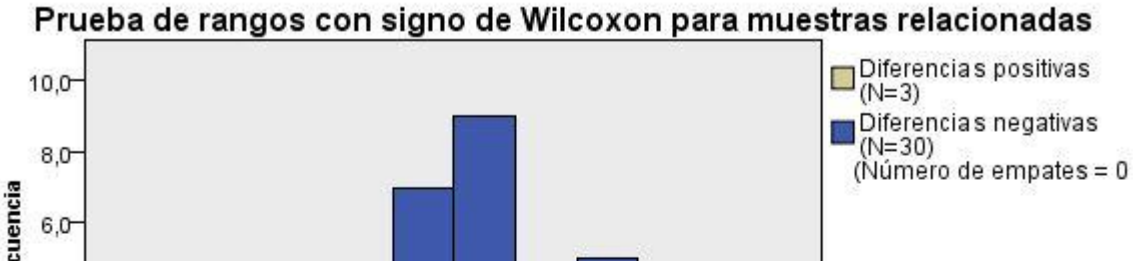
Interpretación: Los resultados de la prueba de Wilcoxon, nos arrojan una media de 19.81 minutos; con una desviación estándar de la muestra de 5.51.

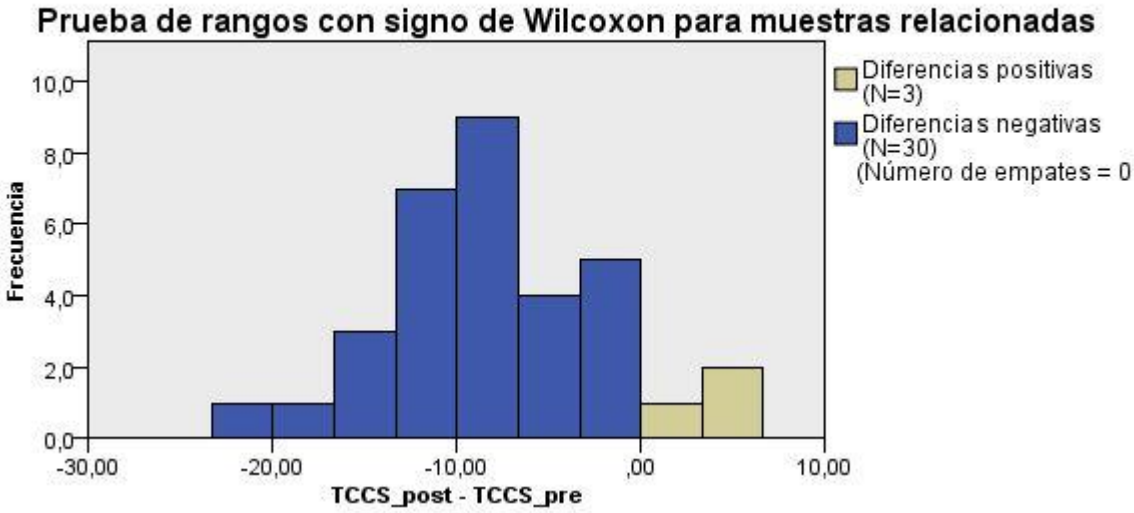
Información de Campo Continuo TSI-pos



Interpretación: Los resultados de la prueba de Wilcoxon, nos arrojan una media de 11.88 minutos; con una desviación estándar de la muestra de 1.613.

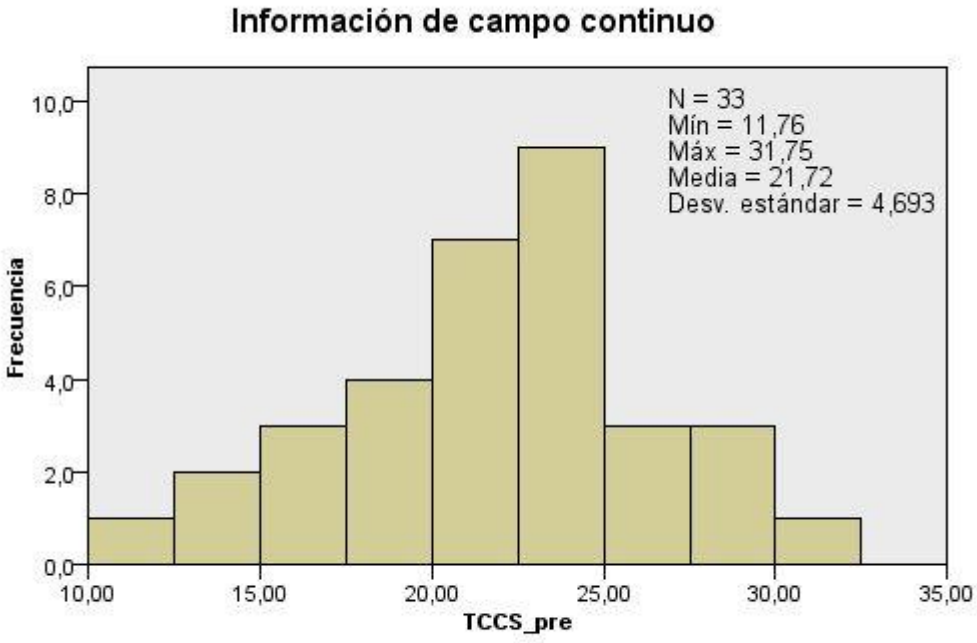
Indicador 2: Tiempo en crear copia de seguridad de la información





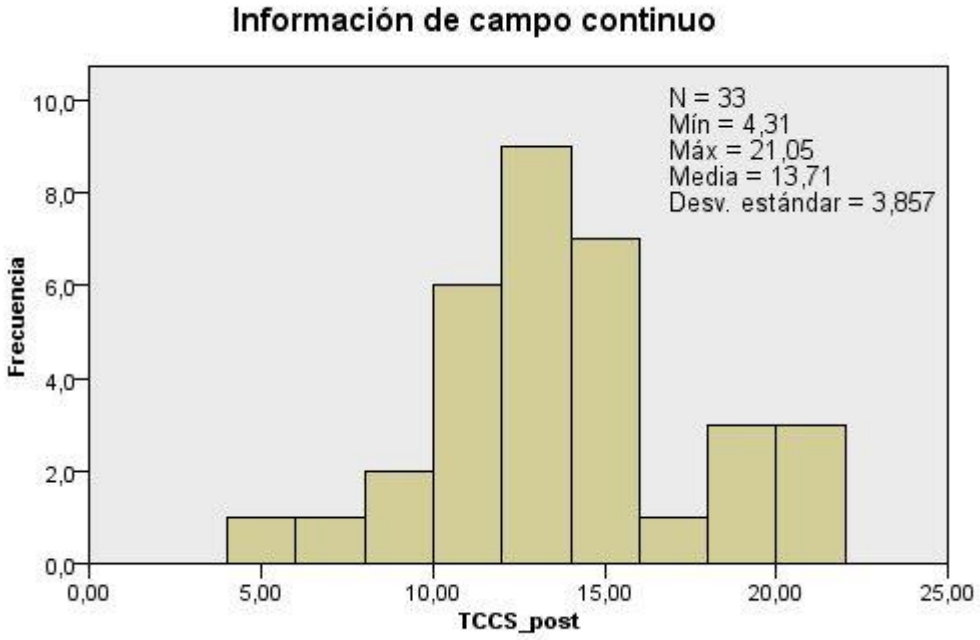
N total	33
Estadístico de contraste	21,000
Error estándar	55,965
Estadístico de contraste estandarizado	-4,637
Sig. asintótica (prueba bilateral)	,000

Información de campo Continuo TCCS_pre



Interpretación: Los resultados de la prueba de Wilcoxon, nos arrojan una media de 21.72 minutos; con una desviación estándar de la muestra de 4.69.

Información de campo Continuo TCCS_post



Interpretación: Los resultados de la prueba de Wilcoxon, nos arrojan una media de 13.71 minutos; con una desviación estándar de la muestra de 3.85.

5.4. Discusión de resultados

Indicador Nº 01: Tiempo Solicitado para la Información

En relación a los resultados de las medias del indicador se tiene que existe una diferencia de 7.93 minutos en favor del Tiempo solicitado para la información, esta diferencia representa una reducción del tiempo de 79.3%.

Indicador Nº 02: Tiempo en crear copia de seguridad de la información

En relación a los resultados de las medias del indicador se tiene que existe una diferencia de 8.01 minutos en favor del ERP, esta diferencia representa una reducción del tiempo de 80.1%.

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones.

Finalizado el presente trabajo de tesis se llegaron a las siguientes conclusiones:

1. Los resultados de la prueba no paramétrica de Wilcoxon para el indicador 1 Tiempo solicitado para la información el Valor p=0,000002 demuestra que existe diferencia significativa entre las muestras relacionadas, entre el antes y el después por lo tanto se aprueba la Hipótesis Alterna Ha1. En relación a los resultados de las medias del indicador se tiene que existe una diferencia de 7.93 minutos en favor del Tiempo solicitado para la información, esta diferencia representa una reducción del tiempo de 79.3%.
2. Los resultados de la prueba no paramétrica de Wilcoxon para el indicador 2 Tiempo en crear copia de seguridad de la información el Valor p=0,000004 demuestra que existe diferencia significativa entre las muestras relacionadas, entre el antes y el después por lo tanto se aprueba la Hipótesis Alterna Ha1.En relación a los resultados de las medias del indicador se tiene que existe una diferencia de 8.01 minutos en favor de crear copia de seguridad de la información, esta diferencia representa una reducción del tiempo de 80.1%.

3. Finalmente, podemos concluir que los resultados de la prueba de Wilcoxon, nos arrojan en el indicador 1 una media de 11.88 minutos;

con una desviación estándar de la muestra de 1.613 y para el indicador 2, nos arrojan una media de 13.71 minutos; con una desviación estándar de la muestra de 3.857.

6.2. Recomendaciones.

Finalizado el presente trabajo de tesis se llegó a las siguientes recomendaciones.

1. *Se recomienda que se lleve a cabo la implementación del proyecto para proteger la integridad del funcionamiento de la red supervisando el trabajo de los servidores y velando por el correcto funcionamiento de las comunicaciones informáticas.*
2. *Garantizar que los servicios implementados sean utilizados para los fines que fueron creados*
3. Comunicar a un especialista en Seguridad Informática los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes.
4. Capacitar al personal encargado en controles de seguridad informática.

REFERENCIAS BIBLIOGRAFICAS

Enlaces:

1. https://www.derechoycambiosocial.com/revista032/auditoria_a_las_tecnologias_de_la_informatica.pdf
2. http://dialnet.unirioja.es/servlet/oaiart?codigo=2059077
3. http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5677/AGUIRRE_DAVID_SISTEMA_GESTION_SEGURIDAD_INFORMACION_SERVICIOS_POSTALES.pdf;sequence=1
4. file:///C:/Users/Downloads/lujan_m.pdf
5. http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/3362/Caballero%20Nu%C3%B1ez.pdf?sequence=1&isAllowed=y
6. https://www.isotools.org/2016/09/06/consiste-sistema-gestion-la-seguridad-salud-trabajo-sg-sst/
7. http://www.umariana.edu.co/dependencias/gestion-talento-humano/index.php/sistema-de-gestion-sst
8. http://www.umariana.edu.co/dependencias/gestion-talento-humano/index.php/sistema-de-gestion-sst
9. http://catarina.udlap.mx/u_dl_a/tales/documentos/msp/murillo_c_sr/capitulo1.pdf
10. https://www.significados.com/seguridad-informatica
11. https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009730_.htm

12. https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009730_.htm

13. https://www.google.com/search?source=hp&ei=oOjQW6SbLoHb5gL41orwBg&q=dise%C3%B1o+experimental&oq=dise%C3%B1o+experimental&gs_l=psy-ab.3..0i131k1j0l9.1547.10207.0.10761.21.13.1.7.7.0.459.2576.2-6j2j1.9.0....0...1c.1.64.psy-ab..4.17.2627...0i10k1.0.Hf9ITeyvkKc

14. MARQUEZ GARCIA, FRANCISCO. 1993. UNIX. Programación Avanzada Addison-Wesley Iberoamericana.

15. SANCHEZ L., ENRIQUE Y RICO G., ANGEL 1994. “Fenix : Sistema para la Administración Integral de UNIX en la UNMSM-P.”

16. CABALLERO, PINO. 1998 “Seguridad Informatica”. Técnicas criptográficas. Computec Ra-Ma. May 1998.

17. Modelo de seguridad informática, gobierno de Quintana Roo, México, Enero 2005.

18. http://www.microsoft.com/latam/windowsserversystem/isaserver/default.mspx

19. Políticas de seguridad informática: Mejores prácticas internacionales: www.scientechsecurity.com, anexo digital.

20. Juan Carlos Oré, Introducción a la seguridad de la información, Junio del 2006 http://www.siicex.gob.pe/siicex/resources/capacitacion/6775ce6a-09a5-4b24-b25a-ad1ab2558cac.pdf

21. Seguridad de la información y el software libre, **The Ska,** Security Specialist http://www.involucrate.org/wp-content/uploads/2007/11/carlos-horna-seguridad-con-software-libre.pdf

22. **http://www.gmv.es/seguridad_informacion/seguridad.htm**

23. http://www.microsoft.com/latam/isaserver

24. Norma estándar británico 7799, http://www.auditoria.com.mx/not/boletin/2005/0510.htm

25. http://dialnet.unirioja.es/servlet/listatesisporclasificacion?tipo_busqueda=UNESCO&clave_busqueda=120317

26. http://dialnet.unirioja.es/servlet/oaiart?codigo=2059077

27. Contribución a la mejora de las técnicas de auditoría informática mediante la aplicación de métodos y herramientas de ingeniería del conocimiento

28. http://www.nobosti.com/spip.php?article69

29. Rafael Ausejo Prieto, Gestión de Proyectos de Auditoria de Seguridad, 2003.

30. CIDETEC, Auditoría Informática, Maestría en Tecnología de Cómputo, Agosto 2008.

31. www.regionica.gob.pe

32. www.itigi.og
33. http://www.itil-officialsite.com/home/home.asp
34. http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981
35. http://es.wikipedia.org/wiki/Normas_ISO_9000

ANEXOS

ANEXO: MATRIZ DE CONSISTENCIA

TITULO: "Modelo de un Sistema de Seguridad Informática Aplicado en la Empresa Municipal de Agua Potable y Alcantarillado de Ica - EMAPICA"

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	INDICADORES	MÉTODOS	TECNICAS E INSTRUMENTOS
Problema Principal	*Objetivo General*	*Hipótesis General*				
PG: ¿En qué medida el modelo de un sistema de seguridad informática influye en mejorar el manejo de la información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA? **PE_1:** ¿En qué medida el modelo de un sistema de seguridad informática influye en mejorar el tiempo solicitado en pedir información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA? **PE_2:** ¿En qué medida el modelo	**OG:** Determinar como el modelo de un sistema de seguridad informática mejora la seguridad de la información en la empresa municipal de agua potable y alcantarillado de Ica. **OE1:** Determinar como el modelo de un sistema de seguridad informática mejora el tiempo solicitado en solicitar información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA. **OE2:** Determinar como el modelo de	**HG:** El diseño de un modelo de seguridad Informática influye en mejorar la información en la empresa municipal de agua potable y alcantarillado de Ica – EMAPICA. **HE1:** El diseño de un modelo de seguridad Informática influye en mejorar el tiempo solicitado para la information en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA. **HE2:** El diseño de un modelo de seguridad Informática influye en mejorar el tiempo en crear copia de seguridad de la	***Variable Independiente(X) :*** Sistema de seguridad informática ***Variable Dependiente(Y) :*** Aplicación del mejoramiento de la información	*Indicadores:* Y_1: Tiempo solicitado para la información Y_2: Tiempo en crear copia de seguridad de la información	Tipo de Investigación: Aplicada Nivel de investigación: Practico Diseño de la investigación: Experimental – cuasi experimental Población : Para el presente proyecto de tesis se utilizó una población de 50 personas entre personal administrativo y el personal del centro de cómputo Muestra : La muestra calculada fue de 33 personas n = 33	TECNICAS • Entrevistas • Análisis • Observación directa INSTRUMENTOS • Guía directa • Guía de entrevista • Guía de observación

de un sistema de seguridad informática influye en mejorar el tiempo en crear copia de seguridad de la información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA?	un sistema de seguridad informática mejora el tiempo en crear copia de seguridad de la información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA	información en la Empresa Municipal de Agua Potable y Alcantarillado de Ica EMAPICA				