



UNIVERSIDAD CATÓLICA LOS ÁNGELES DE
CHIMBOTE

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE
SISTEMAS

IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE
ACCESO A RED EN LA EMPRESA SIMA - CHIMBOTE;
2018.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE
INGENIERO DE SISTEMAS

AUTOR:

BACH. JEHU BENIGNO MARTINEZ CABRERA

ASESORA:

MGTR. ING. MARÍA ALICIA SUXE RAMÍREZ

CHIMBOTE – PERÚ

2018

JURADO EVALUADOR DE TESIS Y ASESOR

DR. ING. CIP. VÍCTOR ÁNGEL ANCAJIMA MIÑÁN
PRESIDENTE

MGTR. ING. CIP. ANDRÉS DAVID EPIFANÍA HUERTA
SECRETARIO

MGTR. ING. CIP. CARMEN CECILIA TORRES CECLÉN
MIEMBRO

MGTR. ING. CIP. MARÍA ALICIA SUXE RAMÍREZ
ASESORA

DEDICATORIA

Con especial cariño a mis padres Benigno y Tereza por inculcarme valores, guía, disciplina y perseverancia lo cual permitió poner el mayor empeño en culminar el presente trabajo de tesis. A mis hermanos Joel y Josué, quienes me apoyaron y motivaron en la continuación de mi carrera universitaria.

Con mucho amor a mi esposa y compañera Janet, que me dio su apoyo, paciencia y comprensión día a día. A mis hijos Benny y Rayner que son el motivo de progreso, sin los cuales habría sido más difícil completar con éxito este trabajo de tesis. A todos ellos los hago parte de este logro profesional.

A todos mis familiares quienes de una u otra forma me motivaron para alcanzar este objetivo.

Jehu Benigno Martinez Cabrera

AGRADECIMIENTO

Agradezco a Dios por bendecir cada día de mi vida con el fin de afrontar los retos con optimismo.

A los directivos de la empresa SIMA - Chimbote por facilitarme el acceso a los ambientes de trabajo y obtener la información requerida para esta investigación, esperando contribuir a la mejora continua de la empresa, así también a los profesionales que me brindaron sus sugerencias y críticas constructivas para el desarrollo de este trabajo.

A la Mg. Ing. María Alicia Suxe Ramírez por su asesoría, paciencia, método didáctico que permitió desarrollar y culminar esta tesis.

Jehu Benigno Martinez Cabrera

RESUMEN

Esta tesis se desarrolló en el ámbito de la línea de investigación denominada: Implementación de las tecnologías de la información y comunicación (TIC) para la mejora continua de la calidad de las organizaciones del Perú, de la escuela profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote; cuyo objetivo fue realizar la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote, con el fin de mejorar el control de las cuentas de usuarios y la seguridad de la red; se basó en el diseño no experimental, fue de corte transversal; la población fue de 10 usuarios y se seleccionó como muestra a los 10 usuarios; se usó el método no probabilístico con muestra por conveniencia; luego de una encuesta se obtuvieron los resultados siguientes: respecto a la dimensión Nivel de satisfacción del actual control de acceso a red, el 50% de usuarios respondió que SÍ está satisfecho por la atención de sus cuentas de acceso a red, en tanto que el restante 50% respondió que NO está satisfecho por la atención; asimismo respecto a la dimensión Necesidad de implementación de un sistema de control de acceso a red, el 100% de usuarios encuestados respondió que SÍ es necesario la implementación de un sistema de control de acceso a red. Estos resultados confirman la hipótesis general, por ello esta investigación se justifica con el fin de implementar un sistema de control de acceso a red en la empresa SIMA – Chimbote.

Palabras clave: Acceso, Control, Red, Sistema.

ABSTRACT

This thesis was developed in the scope of the research line called: Implementation of information and communication technologies (ICT) for the continuous improvement of the quality of organizations in Peru, the professional school of Systems Engineering of the University Catholic Los Angeles de Chimbote; whose objective was to carry out the implementation of a network access control system in the company SIMA - Chimbote, with the aim of improving the control of user accounts and the security of the network; was based on non-experimental design, was cross-sectional; the population was 10 users and the 10 users were selected as a sample; the non-probabilistic method with sample was used for convenience; After a survey, the following results were obtained: Regarding the Satisfaction level dimension of the current network access control, 50% of users answered that YES is satisfied with the attention of their network access accounts, while the the remaining 50% answered that they are NOT satisfied with the service; also regarding the dimension Need for implementation of a network access control system, 100% of users surveyed answered that it is necessary to implement a network access control system. These results confirm the general hypothesis, so this research is justified in order to implement a network access control system in the company SIMA - Chimbote.

Keywords: Access, Control, Network, System.

ÍNDICE DE CONTENIDO

JURADO EVALUADOR DE TESIS Y ASESOR.....	ii
DEDICATORIA	iii
AGRADECIMIENTO	iv
RESUMEN	v
ABSTRACT.....	vi
ÍNDICE DE CONTENIDO	vii
ÍNDICE DE TABLAS	x
ÍNDICE DE GRÁFICOS	xii
I. INTRODUCCIÓN	1
II. REVISIÓN DE LA LITERATURA	4
2.1. Antecedentes	4
2.1.1. Antecedentes a nivel internacional	4
2.1.2. Antecedentes a nivel nacional.....	5
2.1.3. Antecedentes a nivel regional	6
2.2. Bases teóricas.....	8
2.2.1. Los Astilleros en el Perú.....	8
2.2.2. La Empresa SIMA - Chimbote	9
2.2.3. Las Tecnologías de información y comunicaciones (TIC).....	23
2.2.4. Teoría relacionada con la Tecnología de la investigación.....	23
2.2.4.1. Sistema de control de acceso a red	23
2.2.4.2. Servidores	28
2.2.4.3. Seguridad.	30
2.2.4.4. Entornos de desarrollo.	37
III. HIPÓTESIS	50
3.1. Hipótesis General.....	50

3.2. Hipótesis específicas.....	50
IV. METODOLOGÍA.....	51
4.1. Diseño de la investigación.....	51
4.2. Población y Muestra.....	51
4.3. Definición operacional de las variables en estudio.....	53
4.4. Técnicas e instrumentos de recolección de datos.....	55
4.4.1. Técnica.....	55
4.4.2. Instrumentos.....	55
4.5. Plan de análisis.....	56
4.6. Matriz de consistencia.....	57
4.7. Principios éticos.....	60
V. RESULTADOS.....	61
5.1. Resultados.....	61
5.2. Análisis de resultados.....	85
5.3. Propuesta de mejora.....	87
5.3.1. Requerimientos de implementación y desarrollo.....	91
5.3.2. Requerimientos funcionales.....	94
5.3.3. Requerimientos no funcionales.....	95
5.3.4. Casos de Uso.....	99
5.3.5. Interfaces.....	111
VI. CONCLUSIONES.....	141
VII. RECOMENDACIONES.....	142
REFERENCIAS BIBLIOGRÁFICAS.....	143
ANEXOS.....	147
ANEXO NRO. 1: CRONOGRAMA DE ACTIVIDADES.....	148
ANEXO NRO. 2: PRESUPUESTO.....	149

ANEXO NRO. 3: CUESTIONARIO 150

ÍNDICE DE TABLAS

Tabla Nro. 1: Hardware – Equipos cómputo escritorio	19
Tabla Nro. 2: Hardware - Servidores.....	20
Tabla Nro. 3: Hardware - Impresoras	20
Tabla Nro. 4: Hardware - equipos de conectividad	20
Tabla Nro. 5: Software - Servidores según tipo de servicio	20
Tabla Nro. 6: Software - Sistemas de información.....	21
Tabla Nro. 7: Software instalado	22
Tabla Nro. 8: Ciclo de vida de software	37
Tabla Nro. 9: Modelo cascada	39
Tabla Nro. 10: Métodos ágiles.....	42
Tabla Nro. 11: Programación extrema.....	42
Tabla Nro. 12: Resumen de población y muestra.....	52
Tabla Nro. 13: Matriz de operacionalización de la variable Implementación de un Sistema de Control de acceso a red.	53
Tabla Nro. 14: Matriz de consistencia	57
Tabla Nro. 15: Satisfacción por la atención de cuentas de acceso.	61
Tabla Nro. 16: Compartir recursos de la PC.....	62
Tabla Nro. 17: Acceso a puertos USB.....	63
Tabla Nro. 18: Instalar software en la PC asignada.....	64
Tabla Nro. 19: Acceso a internet sin restricciones.	65
Tabla Nro. 20: Políticas de acceso a internet.....	66
Tabla Nro. 21: Cambio de contraseña luego de una reasignación.....	67
Tabla Nro. 22: Cancelación de privilegios.	68
Tabla Nro. 23: Registro de los incidentes de la red.....	69
Tabla Nro. 24: Identificar a los equipos que se conectan a la red.	70
Tabla Nro. 25: Resumen dimensión 1 Nivel de satisfacción.....	71
Tabla Nro. 26: Mejora de control de accesos de usuarios.	73
Tabla Nro. 27: Sistema propuesto amigable de usar.	74
Tabla Nro. 28: Incorporar funciones en el sistema propuesto.....	75
Tabla Nro. 29: Mejorar el actual proceso de control de accesos.....	76
Tabla Nro. 30: Implementar funciones centralizadas.....	77

Tabla Nro. 31: Reportes ágiles que permitan supervisión.....	78
Tabla Nro. 32: Funcionalidad y seguridad.....	79
Tabla Nro. 33: Eficiencia en el control de accesos.....	80
Tabla Nro. 34: Permitir que el mismo usuario cambie su contraseña.	81
Tabla Nro. 35: Notificación vía correo por caducidad de contraseña.	82
Tabla Nro. 36: Resumen dimensión 2: necesidad de implementación.....	83
Tabla Nro. 37: Sistema operativo servidores en SIMA - Chimbote.....	87
Tabla Nro. 38: Sistemas Operativos Clientes en SIMA - Chimbote.....	87
Tabla Nro. 39: Configuraciones existentes.....	88
Tabla Nro. 40: Evaluación IDE Netbeans.....	89
Tabla Nro. 41: Evaluación IDE Eclipse.....	90
Tabla Nro. 42: Evaluación IDE Visual Studio .Net.....	90
Tabla Nro. 43: Requerimientos implementación.....	91
Tabla Nro. 44: Actividades de Control de acceso a red.....	93
Tabla Nro. 45: Requerimientos funcionales.	94
Tabla Nro. 46: Requerimientos no funcionales.	95
Tabla Nro. 47: Requerimientos de hardware y software.	96
Tabla Nro. 48: Definición de actores.....	98
Tabla Nro. 49: Actividades administrador.....	98
Tabla Nro. 50: Actividades Supervisor.....	98
Tabla Nro. 51: Actividades Usuario.	99
Tabla Nro. 52: Actividades Base datos.....	99
Tabla Nro. 53: Casos de uso.....	99
Tabla Nro. 54: Presupuesto implementación del sistema de control.....	139

ÍNDICE DE GRÁFICOS

Gráfico Nro. 1: Ubicación geográfica SIMA - Chimbote	11
Gráfico Nro. 2: Frontis SIMA - Chimbote	13
Gráfico Nro. 3: Organigrama SIMA - Chimbote.....	14
Gráfico Nro. 4: Red de datos fibra óptica y UTP	16
Gráfico Nro. 5: Controles de seguridad	31
Gráfico Nro. 6: La criptografía	32
Gráfico Nro. 7: Triangulo de la intrusión	33
Gráfico Nro. 8: Esquema típico de firewall.....	33
Gráfico Nro. 9: Sistema Kerberos.....	36
Gráfico Nro. 10: Esquema autenticación.....	37
Gráfico Nro. 11: Modelo cascada	39
Gráfico Nro. 12: Desarrollo evolutivo.....	40
Gráfico Nro. 13: Modelo Basado en componentes.....	40
Gráfico Nro. 14: RAD	43
Gráfico Nro. 15: Proceso desarrollo	43
Gráfico Nro. 16: Ejemplo diagrama UML.....	45
Gráfico Nro. 17: Arquitectura de bases de datos	46
Gráfico Nro. 18: SQL server.....	47
Gráfico Nro. 19: Programación C#.....	49
Gráfico Nro. 20: Resumen Dimensión 1	72
Gráfico Nro. 21: Resumen Dimensión 2	84
Gráfico Nro. 22: Esquema del sistema	92
Gráfico Nro. 23: Diagrama de clases.....	97
Gráfico Nro. 24: CU01 Ingresar al sistema.	100
Gráfico Nro. 25: CU02 Requerimiento crear usuario.....	101
Gráfico Nro. 26: CU03 Crear usuario de red.....	101
Gráfico Nro. 27: CU04 Nivel de usuario.....	102
Gráfico Nro. 29: CU06 Verificar vigencia de contraseña.	103
Gráfico Nro. 30: CU07 Controlar acceso a internet	104
Gráfico Nro. 31: CU08 Generar reportes.....	105
Gráfico Nro. 32: CU09 Generar Backup del sistema	105

Gráfico Nro. 33: Diagrama de Secuencia - Ingresar al sistema.....	106
Gráfico Nro. 34: Diagrama de Secuencia – Requerimiento crear usuario.....	106
Gráfico Nro. 35: Diagrama de Secuencia - Crear usuario	107
Gráfico Nro. 36: Diagrama de Secuencia - Asignar nivel de usuario.....	107
Gráfico Nro. 37: Diagrama de Secuencia - Cambiar contraseña.....	108
Gráfico Nro. 38: Diagrama de Secuencia - Verificar vigencia de contraseña.....	108
Gráfico Nro. 39: Diagrama de Secuencia - Controlar acceso a internet.....	109
Gráfico Nro. 40: Diagrama Secuencia – Generar reportes.	109
Gráfico Nro. 41: Diagrama de Secuencia – Generar backup del sistema.....	110
Gráfico Nro. 42: Ingresar al sistema.....	111
Gráfico Nro. 43: Menú de sistema.....	112
Gráfico Nro. 44: Formulario gestión de usuarios	113
Gráfico Nro. 45: Formulario cambiar contraseña.....	114
Gráfico Nro. 46: Formulario Gestión Pc	115
Gráfico Nro. 47: Formulario Control Internet	116
Gráfico Nro. 48: Formulario reportes	117
Gráfico Nro. 49: Diagrama de Flujo de proceso.....	118
Gráfico Nro. 50: Diagrama de Base de Datos	119
Gráfico Nro. 51: Cronograma implementación del sistema.	140

I. INTRODUCCIÓN

El contexto empresarial exige que las redes de datos deben estar controladas y supervisadas para así proteger la información, por ello este trabajo tuvo como guía seguir las buenas prácticas existentes en el campo de la protección de entornos organizacionales, tal como el código ITIL V3, capítulo 3.4, directiva Gestión de la Seguridad de la Información, en el cual se establece que la información sólo debe ser accesible para aquellos clientes y/o usuarios a los que está dirigida (1).

Así también tuvo como guía la norma técnica peruana NTP-ISO/IEC 27001:2014, cláusula A.9.4 que establece la política de control de acceso a redes, cuyos diversos controles mencionan utilizar mecanismos de autenticación para controlar el acceso de los usuarios (2).

Se identificó la situación problemática siguiente: el control de cuentas de acceso a red es gestionada manualmente por el administrador de red, quien sincroniza manualmente el acceso, vía escritorio remoto, en el servidor Active Directory, en los servidores Linux de aplicaciones y de correo; también se encontró que las contraseñas de acceso de los usuarios a red no son cambiados periódica e interactivamente por los usuarios, de acuerdo a recomendaciones vigentes, encontrándose que algunas contraseñas datan de hace 02 años. Esta situación observada no contribuye a la seguridad de las cuentas y de la red.

Debido a esta situación problemática se planteó el siguiente enunciado del problema: ¿Con la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote, en el año 2018, mejorará el control de las cuentas de usuarios y la seguridad de la red?

A fin de solucionar esta situación problemática se definió el siguiente objetivo general: realizar la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote, con el fin de mejorar el control de las cuentas de usuarios y la seguridad de la red.

En consecuencia con el fin de alcanzar el objetivo general se definieron los siguientes objetivos específicos:

1. Realizar evaluación tecnológica de la plataforma de servidores Linux y Windows que brindan los servicios informáticos, y también de la plataforma de computadoras clientes.
2. Realizar evaluación de las configuraciones existentes en los servidores Active Directory, Linux y Windows, con el fin de establecer el alcance y limitaciones del Sistema propuesto, para no alterar el funcionamiento de los Sistemas de Información desarrollados en la empresa.
3. Realizar evaluación del entorno de desarrollo más apropiado que permita la centralización e interacción del sistema de control de acceso con el servidor Active Directory y los servidores Linux.
4. Desarrollar la propuesta de implementación del sistema de control de acceso a red en la empresa SIMA - Chimbote, 2018, con el fin mejorar el control de las cuentas de usuarios y la seguridad de la red.

Esta investigación tuvo justificación académica basada en que contribuyó sustancialmente a mi formación integral como Ingeniero de Sistemas ya que permitió afianzar y poner en práctica, en ambientes de producción, los conocimientos adquiridos a lo largo de 10 ciclos académicos en la Universidad Católica Los Ángeles de Chimbote.

Tuvo justificación operativa porque fue factible implementar el sistema de control de acceso ya que los conocimientos requeridos fueron viables y se logró mayor productividad al tener automatizado el control de acceso mejorando la gestión TI. Como justificación económica se tuvo que la implementación de este proyecto permitió ahorro de tiempo y costos operativos al sistematizar el control de acceso de usuarios; el beneficio económico que se obtuvo fue proporcional al nivel de sistematización en el área TI.

La justificación tecnológica fue que esta implementación brindó a la empresa un sistema automatizado aplicado a la reducción de tiempo empleado en procesos repetitivos con el fin de concentrarse aún más en las actividades de producción.

La justificación institucional se basó en que el SIMA - Chimbote al tener certificaciones de índole internacional como ISO 14000:2004 e ISO 18001:2007, otorgado por SGS (3), y Normas y Estándares BASC, otorgado por World BASC Organization (4), necesita sistematizar progresivamente sus procesos TI.

El alcance de la investigación abarca el beneficio directo para la división de tecnologías de la información y comunicaciones del SIMA - Chimbote, por ser la encargada de realizar las tareas de administración de sus áreas clientes como la Jefatura Simach, Oficina Financiera, Oficina logística, Oficina Gestión Integrada, Oficina Seguridad y Salud, Jefatura Departamento de Producción, Jefatura de División Astillero, División Diseño y Desarrollo, División Control de la Producción, División de Control de Calidad y Talleres de producción.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

En el año 2016, los autores Balsero A. y Vargas C. (5), presentaron su tesis titulada “Diseño e Implementación de un Prototipo para el Control de Acceso en la sede de Ingeniería de la Universidad Distrital Francisco José de Caldas mediante el uso de torniquetes controlados por carnet con tecnología NFC y lector biométrico de huella dactilar”, desarrollado en Bogotá, Colombia, en el cual emplearon como metodología la observación del sistema existente, la investigación de literatura para mejorar el control, luego investigación y evaluación de casos de éxito similares con productos comerciales; luego de pruebas con prototipos concluyeron que permitió automatizar la seguridad y el control de accesos, recomendaron a la institución acoger el proyecto en base a costo reducidos.

En el año 2015, el autor Ahumada D. (6), en su tesis titulada “Sistema De Control de Acceso para un Endpoint”, realizado en Chile, refiere que usó como metodología de investigación la observación, cuestionario al usuario y contacto con investigadores del extranjero que habían desarrollado en esa misma área; concluyó que permitió controlar el acceso a los datos de un endpoint, que es un servicio web que permite consultas estructuradas; fue genérica ya que los accesos se hicieron mediante http y fue interactivo para el usuario; luego recomendó administrar varios endpoint con la misma interfaz.

En el año 2014, el autor Cano J. (7), en su tesis de grado “Implementación del Sistema Centralizado de Autenticación y Autorización para las Aplicaciones Web del Centro de Cálculo e

Investigación de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala”, en Guatemala, usó el método de investigación de campo y revisión de literatura, evaluó varias herramientas open source que cumplieran con la funcionalidad; seleccionó la herramienta OpenAM; obtuvo como resultado una plataforma que aseguró las aplicaciones web en forma segura y escalable; permitió integrarse con otros servicios de nube, permitió centralizar la administración de usuarios y credenciales; finalmente recomendó realizar análisis de los recursos que deben ser asegurados y los que pueden ser públicos.

2.1.2. Antecedentes a nivel nacional

En el año 2017, Blas J. (8), en su tesis “Seguridad y control del acceso a las redes inalámbricas en la UNSM-T mediante servidores de autenticación Radius con el uso de Certificados Digitales”, en Tarapoto, Perú, usó como técnicas para la recolección de datos la observación, reportes de la solución implementada, la encuesta, así como software de simulación y medición de indicadores de red; concluyó que luego de la implementación se minimizó el riesgo de los robos de información y ataques a la red, se logró cubrir las deficiencias de seguridad en la red inalámbrica de la UNSM-T, obteniendo excelentes resultados después de la investigación; recomendó la implementación de servidores de acceso inalámbrico al servicio de internet basado en protocolos de seguridad Radius.

En el año 2016, Rivas M. (9), en su tesis de grado “Implementación de un sistema de control de acceso para mejorar la seguridad de la información de la empresa SNX S.A.C.”, Lima, Perú, usó la metodología de investigación de tipo descriptiva, abarcó el estudio sobre los modelos de control de acceso más relevantes, adecuó el modelo de control de acceso seleccionado al escenario en cuestión,

concluyó que un sistema de control de acceso desarrollado en Linux es la opción más adecuada, así también recomendó integrar más servicios desplegados sobre plataforma Linux o Unix, a una red de Microsoft que cuente con Active Directory desplegados en sus versiones más actuales.

En el año 2014, los autores Díaz J. y Salcedo J. (10), en su tesis “Sistema de Prevención de Intrusos para mejorar la seguridad de los servidores de la Universidad Nacional de Trujillo”, usaron como técnicas de recolección de datos las entrevistas, cuestionarios, observación, búsqueda de literatura; concluyeron que a través de su trabajo basado en software la institución obtendría control sobre los posibles ataques de vulnerabilidad a sus servidores, a la vez que se tendría reportes estadísticos, obtuvieron como resultado mayor protección a la red de servidores.

2.1.3. Antecedentes a nivel regional

En el año 2017, los autores Zuñiga M. y Guevara L. (11), en su tesis “Diseño e implementación de un sistema en plataforma Web y Android para control de acceso en la empresa minera Antapaccay”, Arequipa, Perú, propusieron implementar un sistema de control de acceso por software usando herramientas de programación C# para la gestión de pases a un centro minero, emplearon la encuesta para conocer la satisfacción del usuario, fue explicativa, de tipo experimental; mencionaron que obtuvieron resultados satisfactorios, ya que incidió positivamente en la automatización del control de acceso, el tiempo promedio de registro de las unidades se redujo, a la vez que aumentó el grado de satisfacción de los directivos; recomendaron realizar varias pruebas antes de implementar la solución.

En el año 2016, el autor Alfaro M. (12), en su tesis “Sistema de Autenticación por Huella Digital para la Generación de Reportes sobre el Recurso Humano de la Institución Educativa Los Sauces”, Trujillo, Perú, empleó la investigación descriptiva, con cuestionarios antes y después de la implementación del sistema como instrumento de recolección de datos, obtuvo resultados que evidenciaron mejoras en la gestión del recurso humano, rapidez y automatización del proceso, concluyó que hay factores que pueden afectar la correcta ejecución de este procedimiento como son la edad del usuario y las enfermedades de la piel, los cuales deben tomarse en cuenta para asegurar una correcta realización de este proceso, así también expuso recomendaciones como guardar los registros de Base de Datos en la nube digital para mantener la seguridad de dichos datos, realizar un análisis detallado de las relaciones entre las tablas de la Base de datos para contar con información consistente y rápida.

El año 2015, los autores Candia M. y Chavez D. (13), en su tesis “Sistema que permite el control de accesos y el uso de recursos de los usuarios en la biblioteca virtual de la universidad católica de santa maría aplicando la metodología de desarrollo extreme Programming”, Arequipa, Perú, tuvieron el objetivo de controlar las actividades de las computadoras de la biblioteca, concluyeron que con este sistema el administrador es capaz de gestionar las computadoras de los usuarios tales como: visualizar escritorio, controlar escritorio remoto, apagar, reiniciar, cerrar sesión, además pudo interactuar con los usuarios enviando mensajes y compartiendo archivos; luego recomendaron la implementación de una función que capture las palabras digitadas por el usuario; con el fin que se apliquen las técnicas de minería de texto para almacenar datos clave, acontecimientos y otros a fin de establecer los hábitos y preferencias de los usuarios.

2.2. Bases teóricas

2.2.1. Los Astilleros en el Perú

- Concepto.- Realizan actividades relacionadas con la industria naval y en algunos casos relacionados con la industria metal mecánica, lo cual como industria estratégica impulsa el desarrollo socio-económico del país, ya que genera la creación de industrias nacionales en las ramas de las pinturas, soldaduras, ferretería, aceros, equipos auxiliares, motores eléctricos, bombas, carpintería y otras que generan empleo de personal como ingenieros navales, mecánicos, electricistas, arquitectos navales, dibujantes, proyectistas, técnicos, soldadores, pintores, tuberos, etc. Los astilleros se dedican a las actividades de construcción, reparación, modificación estructural y mantenimiento de embarcaciones, según lo requiera el sector estatal, privado, a nivel nacional e internacional (14).

- Historia de los Astilleros.- En el Perú el origen de los astilleros es diverso, tal es el caso del SIMA - Chimbote, Centro de Operación N° 3 del SIMA Perú, que inicia sus actividades el 1° de Marzo de 1975 como Complejo Calderero Estructural de Chimbote para el desarrollo de la Industria Metal Mecánica; luego en 1977 el astillero PICSA de propiedad del Grupo Banquero es transferido al SIMA, integrándose al SIMA - Chimbote (15). El Astillero TASA, en el 2007 inicia actividades en Chimbote, adquiriendo la empresa INASA en cuyas instalaciones realiza trabajos en sus diferentes líneas de negocio con su propia supervisión y control de calidad (16). El astillero Construcciones Maggiolo fue constituido en 1942, por Don Augusto Maggiolo Cavenecia, en la zona de Chucuito, en el puerto del Callao; a fines de los años 50 entregó una serie de Patrulleras a la Marina Peruana; a inicios de la década del año 2000 se llevaron a cabo construcciones de embarcaciones pesqueras con

sistemas de refrigeración en bodegas RSW y diversos proyectos de ampliaciones de embarcaciones (17).

- Tipos de Astilleros.- Se distinguen los que realizan:
La construcción de Alto Bordo: buques mayor o igual a 2,000 toneladas de peso muerto. La Construcción de Bajo Bordo: buques menores a 2,000 toneladas de peso muerto y mayor a 300 toneladas de peso muerto. Las Reparaciones Navales y demás actividades de las industrias conexas que vincula la fabricación de insumos nacionales para la construcción y/o reparación de buques (14).
- Estadísticas de Astilleros.- Como referencia, en el mundo, la clasificación de los diez astilleros con las mayores carteras de pedidos se localiza en el continente asiático, en China, Japón y Corea del Sur. En el Perú la industria de la Construcción Naval de Bajo Bordo está conformada principalmente por cuatro organizaciones: Servicios Industriales de la Marina S.A - SIMA Perú, con sus centros operativos SIMA - Callao y SIMA - Chimbote en la costa y uno ubicado en la Amazonía SIMA - Iquitos. Construcciones Maggiolo S.A., astillero privado familiar ubicado en el Callao. TASA astillero privado ubicado en la costa norte, Chimbote; y Astillero Henry E.I.R.L., empresa privada ubicada en la Amazonía. Estos astilleros brindan servicios principalmente en la construcción de embarcaciones remolcadoras, barcasas y pesqueras (14).

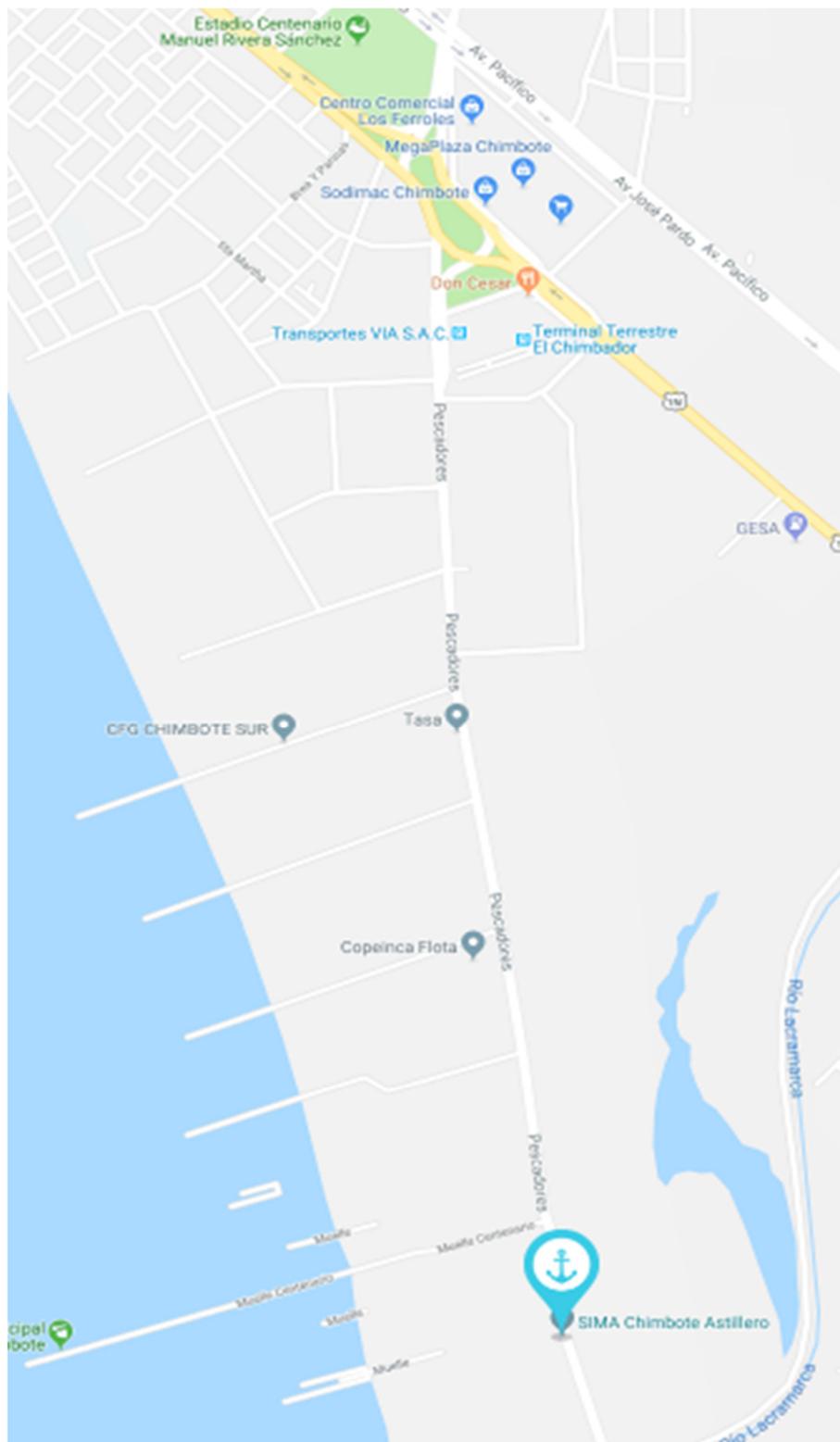
2.2.2. La Empresa SIMA - Chimbote

Información general.-

El SIMA - Chimbote como empresa integrante de Los Servicios Industriales de la Marina S.A., trabaja para contribuir con la defensa nacional, el desarrollo económico y tecnológico del país, ejecutando

grandes proyectos en la industria naval y metalmecánica. Como empresa estatal de derecho privado funciona de acuerdo a la política del ministerio de defensa, de la comandancia general de la marina y del fondo nacional de financiamiento de la actividad empresarial del estado. El centro de operación SIMA - Chimbote es el mayor astillero en el Perú para naves de bajo bordo y uno de los principales centros de producción de estructuras metálicas, el astillero cubre un área de 164,000 m², cuenta con un Sincroelevador de naves, parqueaderos múltiples y talleres, donde se construyen y reparan embarcaciones de hasta 940 toneladas; el centro de producción metal mecánica cuenta con infraestructura propia en un área de 70,000 m², y una gran nave de producción de 10,000 m². El centro de operación SIMA - Chimbote está ubicado en Avenida Los Pescadores 151, Zona Industrial 27 de Octubre, Chimbote, Provincia del Santa, Región Ancash, a 425 kms. al norte de la ciudad de Lima (15).

Gráfico Nro. 1: Ubicación geográfica SIMA - Chimbote



Fuente: Google Maps (18).

Historia.-

El 14 de febrero de 1950, durante el Gobierno de Manuel A. Odría, se crea, la empresa Servicio Industrial de la Marina, conocida como SIMA, se asignó la administración del dique seco y de los talleres existentes, con la finalidad de atender completamente a la Armada, a la Marina Mercante Nacional y entidades privadas. El 1° de Marzo de 1975, se inicia la construcción del Complejo Calderero Estructural de Chimbote y se crea el Centro de Operación N° 3, SIMA - Chimbote para el desarrollo de la Industria Metal Mecánica. En 1977, el astillero PICSA de propiedad del Grupo Bancharo es transferido al SIMA, integrándose a SIMA - Chimbote, especializándose en la construcción, reparación y modernización de embarcaciones pesqueras de hasta 900 toneladas (15).

Objetivos organizacionales.-

En su plan estratégico está el objetivo financiero de alcanzar los niveles de rentabilidad, atraer, retener clientes y grupos de interés mejorando su nivel de satisfacción, fortalecer su imagen empresarial en la comunidad, modernizar y maximizar la capacidad de servicio indicado en la renovación de maquinarias y equipos de producción. Los objetivos en Tecnologías de la Información se plantea mejorar la infraestructura informática de acuerdo a la adecuada planificación de recursos informáticos, los que son medibles en el grado de cumplimiento y satisfacción del usuario en los servicios informáticos de la empresa, además busca optimizar la calidad de la información a través de implementar soluciones TIC que soporten o mejoren los procesos a fin de tener información actualizada de cada área de la organización (15).

Las funciones de la empresa son efectuar en forma prioritaria la reparación, carena, modificación y construcción de los buques de la

Marina de Guerra del Perú, Marina Mercante Nacional y clientes particulares nacionales y extranjeros, promover el desarrollo social, cultural, profesional de sus trabajadores. La división de tecnologías es responsable del desarrollo de aplicativos, mantener la operatividad de los equipos informáticos, evaluar los riesgos inherentes a la actividad teniendo en cuenta la normativa de la empresa.

Visión.-

La empresa tiene como visión ser reconocido como el mejor astillero naval en Latinoamérica, orgullo de la industria Peruana.

Misión.-

La misión es contribuir con la Defensa Nacional, el desarrollo socio-económico y tecnológico del país, liderando proyectos tanto en industria naval como en metalmecánica (15).

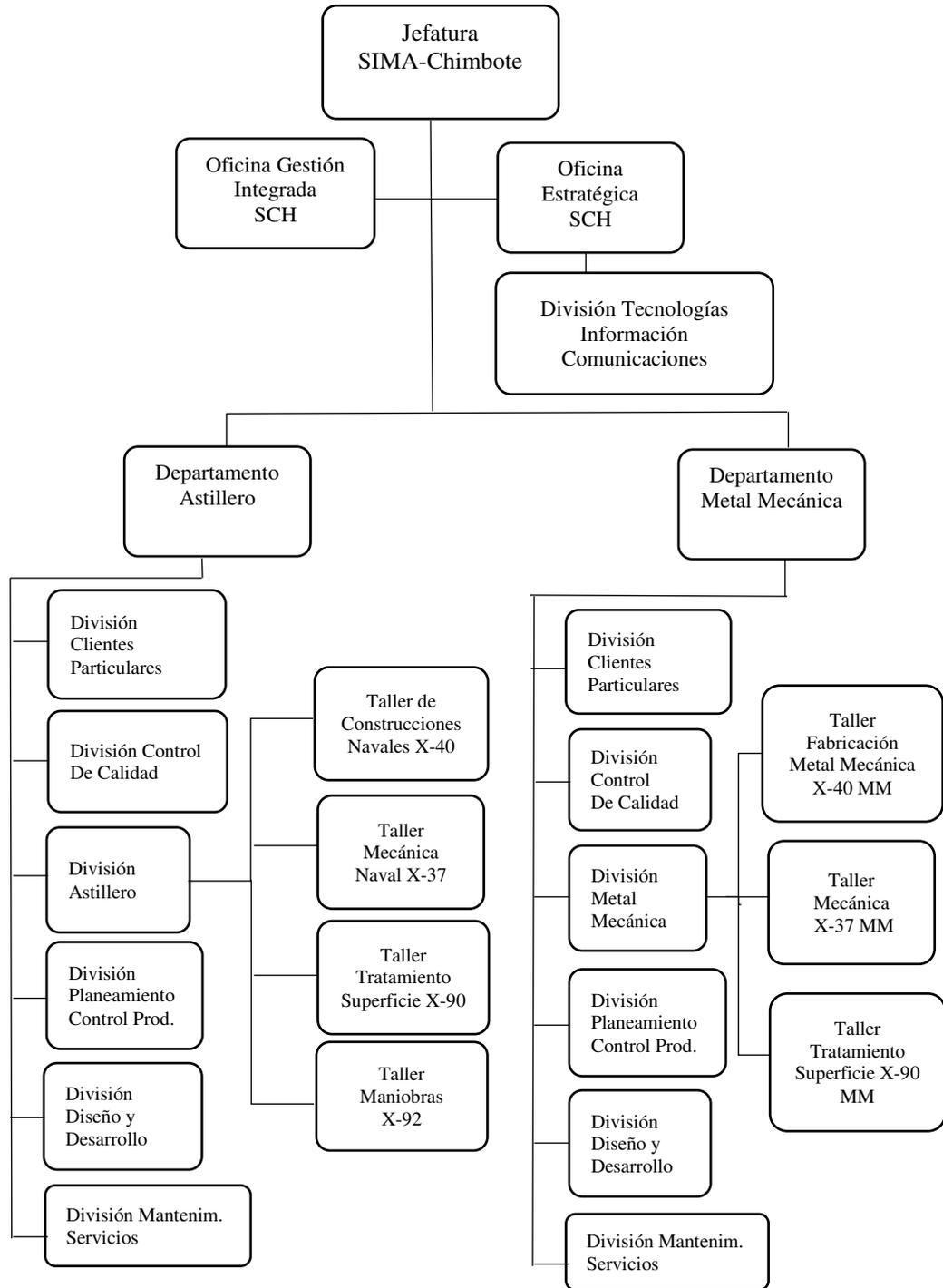
Gráfico Nro. 2: Frontis SIMA - Chimbote



Fuente: SIMA – Chimbote (15).

Organigrama.-

Gráfico Nro. 3: Organigrama SIMA - Chimbote



Fuente: SIMA – Chimbote (15).

Definición.-

Las Tecnologías de la Información y Comunicaciones son el grupo de servicios, redes, software y dispositivos de hardware que se agrupan en sistemas de información que se encuentran interconectados con el objetivo de gestionar datos, información y procesos de modo efectivo, permite aumentar la productividad de los ciudadanos, gobierno, y empresas, posibilitando mejoras en la calidad de vida (19).

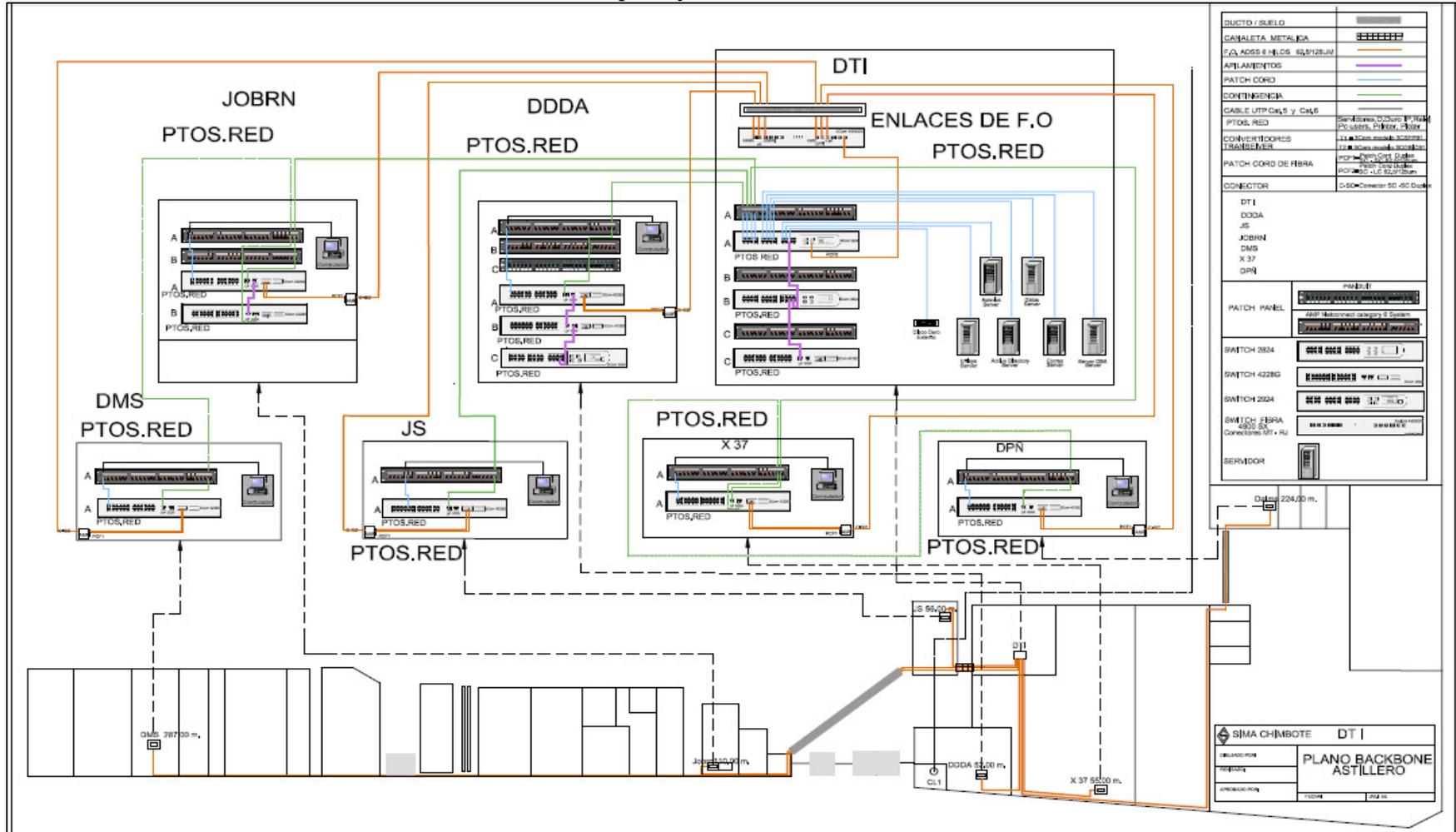
Historia de las TIC en la empresa investigada.-

Las TIC cumple un rol protagónico en la empresa. Tuvo sus inicios en el año 1992 con personal egresado de la Universidad Federico Villareal, que luego fue ampliándose a profesionales de la UNT, quienes iniciaron la red de cómputo con la tecnología Intel 386, Sistema Operativo MS-DOS. En el problema computacional del año 2000 contrataron a más personal ampliándose también la red de usuarios. En la actualidad tiene en servicio diversos sistemas de información desarrollados localmente. Jerárquicamente depende de la Oficina Estratégica, tiene a su cargo personal que realiza labores de Desarrollo de Software y Soporte Técnico. Tiene por misión planear, organizar, implementar, operar y controlar los sistemas de información y comunicaciones. Su visión es proyectar una cultura institucional de modernidad tecnológica en el marco de la gestión de seguridad de la información

TIC que utiliza la empresa investigada.-

Redes de datos.- Compuesta por red backbone de fibra óptica multimodo 50µm MM, que interconecta el switch core principal con switch de distribución y borde, también cableado estructurado UTP Cat6 para la interconexión con las estaciones usuarias.

Gráfico Nro. 4: Red de datos fibra óptica y UTP



Fuente: SIMA – Chimbote (15).

Sistemas de información.- Compuesta por los Sistemas desarrollados en la empresa. Tales como:

Sistema Contabilidad General.- Conjunto de elementos que registran la información financiera y las interrelaciones de estos datos. Esta estructura, por sus características, contribuye a la toma de decisiones en el ámbito de la gerencia. Los sistemas contables se componen de diversos tipos de documentos e implican la participación de contadores que se encargan del registro preciso y del análisis de la información. Los contadores suelen trabajar en conjunto con los gerentes o los responsables de tomar las decisiones de la empresa.

Sistema de Personal.- El Sistema de Personal permite realizar: ingreso y modificación de datos de trabajadores, totalmente compatible con requerimientos laborales y del PDT, ingreso y modificación de datos de personas dependientes de los trabajadores, dispone de mantenimiento de archivos diversos totalmente personalizables de AFP y ONP, Bancos, Conceptos de Planilla, Constantes internas, documentos adjuntos, SCTR, controla qué documentos presenta el trabajador al iniciar su labor en la empresa.

Sistema de Producción.- Es un sistema de información que permite realizar lista de todos los materiales necesarios para hacer el trabajo encomendado. Una relación completa del trabajo a realizar, dividido en número de horas para cada tipo de trabajo especializado. Un plan detallado de secuencia cronológica, que indique cuando deberá trabajar cada tipo de mano de obra y cuándo cada tipo de material deberá estar disponible para poder ser utilizado. Es el sistema en el cual la producción se hace por unidades o cantidades pequeña, cada producto a su tiempo lo cual se modifica a medida que se realiza el trabajo. El proceso productivo es automatizado y estandarizado.

Sistema Parquadero.- Permite localizar en tiempo real la ubicación y estado de atención de las embarcaciones pesqueras en el patio de maniobras. Asimismo permite realizar los presupuestos inherentes a la actividad de carenado, pintado propios de la actividad.

Sistema Gestión de la Calidad.- Es un sistema de información que permite realizar la actividad de control de calidad en las construcciones de naves, reparaciones de estructuras navales, documentando adecuadamente a través de registros de calidad los trabajos de soldaduras de planchas, monitoreo de la actividad de control de calidad con instrumentos tecnológicos.

Sistema Comercial.- Brinda soporte en el presupuesto detallado de las actividades al ingreso/salida, varada/desvarada de embarcaciones pesqueras en la empresa SIMA - Chimbote.

Sistema Logístico.- Permite la gestión centralizada de tareas, como el seguimiento de los niveles de inventario y la ubicación de existencias. El objetivo del sistema de gestión de almacenes es proporcionar la información necesaria para controlar eficientemente el movimiento de materiales dentro de un almacén.

Sistema de Mantenimiento.- Es una herramienta de planificación y control para la gestión eficaz del mantenimiento de los equipos y maquinarias, tiene como objetivo maximizar la productividad y controlar los costos. Los beneficios son: reducir los tiempos de parada de los equipos, reducción en reparaciones, reducción de horas extras de trabajo y tiempo perdido, planificación en la utilización del personal.

Sistema de Solicitud de Útiles y Material de Oficina.- Este sistema permite la actividad de retiro de todo tipo de materiales del almacén

central: materiales de oficina, de soldadura, planchas metálicas, posibilita la actividad productiva.

Sistemas de Archivo Digital.- Permite ingresar, documentar todos los tipos de archivos generados en procesos productivo, sean boletas de ingreso, salida de embarcaciones, boletas de remuneraciones del personal, documentación financiera.

Sistemas de Seguridad.-

Compuesta por Sistema Video Vigilancia IP, que permite la vigilancia electrónica del perímetro de la empresa y del interior controlando puntos claves como puerta de acceso central, zona de tránsito vehicular, tránsito peatonal, almacenes, patio de naves y zona muelle. El cual es registrado en video y almacenado en discos duros por la División de Tecnologías.

Infraestructura tecnológica.-

La empresa presenta equipamiento tecnológico según se muestra en las siguientes tablas:

Tabla Nro. 1: Hardware – Equipos cómputo escritorio

EQUIPOS DE COMPUTO	Tipo de procesador de computadora	Tipo de equipo de computo		Total
		Estaciones de trabajo	Portátil	
	Pentium IV	30	1	31
	Core 2 Duo	65	5	70
	Core 2 Quad	4	-	4
	Core i5	107	9	116
	Core i7	61	-	61
	Total	267	15	282

Fuente: SIMA – Chimbote (15).

Tabla Nro. 2: Hardware - Servidores

	Tipo de tecnología	Cantidad
	Xeon quad core 3.0 GHZ, 24 GB Ram, DD 370 GB	9
	Total	9

Fuente: SIMA – Chimbote (15).

Tabla Nro. 3: Hardware - Impresoras

	Tipo de impresión			
	Matricial	Laser	Inyección	Multifunción
Total	58	16	15	24

Fuente: SIMA – Chimbote (15).

Tabla Nro. 4: Hardware - equipos de conectividad

Equipos de conectividad LAN	Switch	Router	Access Point
Total	34	-	34
Equipos de conectividad WAN	Switch	Router	Access Point
Total	-	2	-

Fuente: SIMA – Chimbote (15).

Tabla Nro. 5: Software - Servidores según tipo de servicio

	Tipo de servicio				
	Aplicaciones web	Aplicaciones de escritorio	Base datos	AD	Correo
Total	1	2	2	2	2

Fuente: SIMA – Chimbote (15).

Tabla Nro. 6: Software - Sistemas de información

Nombre del sistema	Herramientas de TI		
	BD	Servidor BD	Lenguaje de Programación
Modulo control planta	Microsoft SQL server	Windows server 2008	Java
Sistema de Producción	Microsoft SQL server	Windows server 2008	Actionscript
Sistema de Personal	Fox pro	Linux CentOS	Otro
Sistema de Backup	Microsoft SQL server	Windows server 2008	Actionscript
Sistema de Gestión de la Calidad	Microsoft SQL server	Microsoft SQL server	Otro
Sistema de Parquadero	Microsoft SQL server	Windows server 2008	Actionscript
Sistema Comercial	Microsoft SQL server	Windows server 2008	Actionscript
Sistema Logístico	Fox pro	Linux CentOS	Otro
Sistema de Registro de Guías de Remisión	Fox pro	Linux CentOS	Otro
Sistema de Mantenimiento	Fox pro	Linux CentOS	Otro
Sistema de Contabilidad General	Fox pro	Linux CentOS	Otro
Sistema de Contabilidad y de Costos	Fox pro	Linux CentOS	Otro
Sistema de Facturación y Tesorería	Fox pro	Linux CentOS	Otro
Sistema de control patrimonial	Fox pro	Linux CentOS	Otro
Sistema de pañol de herramientas	Microsoft SQL server	Windows server 2013	PHP
Sistema de Solicitud de Útiles y Mat. De Oficina	Microsoft SQL server	Windows server 2008	Actionscript
Sistema de Archivo Digital	Microsoft SQL server	Windows server 2008	Java

Fuente: SIMA – Chimbote (15).

Tabla Nro. 7: Software instalado

Tipo de Software	Herramientas de TI
Sistema Operativo Desktop	Windows xp Profesional
	Windows vista Business
	Windows 7 Profesional
	Windows 8 Profesional
Sistema Operativo Servidores	Windows Server 2008 R2
	Windows Server 2012 R2
	Windows Server 2016 R2
	Linux CentOS 5.8
	Linux CentOS 6.4
Software Desarrollo	Linux Freebsd
	Foxpro 3.0
	Visual Basic 6
	Ms SQL server 2008
	Power Builder 11
	Delphi
Diseño CAD	IDE Netbeans 8.1
	Autocad Lt 2002
	Autocad Lt 2004
	Autocad Lt 2005
	Autocad Lt 2010
	Autocad Lt 2013
	Autoship 8
	Autohydro 8
	Autoplate 8
	Autostructure 3
	Intellicad 2001
	Solidworks 2012
	Algor
	SAP 2000
	Rhinoceros 4
	Orcad 4
	Penguin 4
	Sokia link
	Solid Edge
	DSP Data Management
Ofimática	Ms office 2003
	Ms office 2007
	Ms office 2010
	Ms office 2013
	Ms Project 2003
	Ms Project 2007
	Ms Project 2010
Ms Project 2013	

	OpenOffice 4
Utilitarios	Adobe Acrobat Reader 11
	7-zip
	CutePDF
	VLC
Antivirus	ESET Smart Antivirus

Fuente: SIMA – Chimbote (15).

2.2.3. Las Tecnologías de información y comunicaciones (TIC)

La empresa SIMA - Chimbote acoge las mejores prácticas de la norma técnica peruana NTP-ISO/IEC 27001:2014, anexo A, dominio 9, sobre Control de acceso. Ello está en función de las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño y estructura de la organización que fomenta la presidencia del consejo de ministros a través de la oficina nacional de gobierno electrónico e informático (ONGEI) rige la actividad de las empresas estatales, apoya la modernización de las organizaciones públicas con un enfoque más agudo en seguridad de la información (2).

2.2.4. Teoría relacionada con la Tecnología de la investigación

2.2.4.1. Sistema de control de acceso a red

- Definición.-

Es un sistema automatizado que posibilita en forma eficiente, aprobar o denegar el acceso a determinados entornos de red, basado en la identificación previamente verificada que permite acceder a datos o recursos. Estos sistemas de controles de acceso pueden tomar diversas formas y para múltiples aplicaciones. Por ejemplo, existen sistemas de controles de acceso por software cuando digitamos una contraseña para

abrir el correo, otro ejemplo es al colocar nuestra huella en un lector para encender el PC. Todos ellos permiten el acceso a datos, se integra a través de una PC local o remoto, por medio del uso de un software de control permitiendo registrar todas las operaciones realizadas sobre el sistema con fecha, horario, autorización, etc. Se identifican tres componentes: mecanismo de autenticación que puede ser una clave; mecanismo de autorización, que es la que permite el acceso o no, y mecanismo de trazabilidad, que complementa el de autorización. Son aplicaciones sencillas o sistemas muy complejos y sofisticados (20).

- Clasificación.-

Sistemas de control de acceso en red: son los que se integran mediante el uso de un software que permite registrar todas las actividades realizadas en un determinado sistema.

Sistemas de control de acceso autónomos: son sistemas que permiten el control de puertas, horarios o identificación mediante claves o biometría.

- Características.-

Presenta interacción entre un sujeto y un objeto que permite flujo de información entre ellos. El sujeto es la entidad que recibe o modifica la información, puede ser un usuario, programa, proceso, etc. El objeto es la entidad que suministra o contiene la información y/o datos, que puede ser un fichero, una base de datos, una computadora, un programa, una impresora o un dispositivo de almacenamiento. Estos roles de sujeto y objeto pueden intercambiarse en dos entidades que se

comunican para cumplir una tarea, como pueden ser un programa y una base de datos o un proceso y un fichero. Generalmente consta de una base de datos, un aplicativo desarrollado y los soportes de autenticación a través de servidores.

- Técnicas de identificación y autenticación.-

La identificación se refiere a la acción por el usuario de presentar su identidad a un sistema, generalmente se usa un identificador de usuario. Ello establece que el usuario es responsable de las acciones que lleve a cabo en el sistema. Se relaciona con los registros de auditorías que permiten guardar las acciones realizadas dentro del sistema y rastrearlas hasta el usuario autenticado.

Autenticación es la verificación de la validez de las credenciales que presenta el usuario, generalmente se asigna una contraseña en el momento de iniciar una sesión. Hay cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las que pueden ser usadas en forma individual o combinada denominándose autenticación de varios factores:

Lo que el usuario conoce: ejemplo una contraseña.

Lo que el usuario posee: ejemplo una tarjeta magnética.

Lo que el usuario es y que lo identifica unívocamente: ejemplo las huellas digitales.

Lo que únicamente el usuario es capaz de hacer: ejemplo los patrones de escritura.

La fortaleza de la autenticación es mayor mientras más factores se adicionen, generalmente solo se utilizan hasta 3 factores:

1 factor = contraseña

2 factores = contraseña + token

3 factores = contraseña + token + biometría

4 factores = contraseña + token + biometría + localización geográfica (GPS)

5 factores = contraseña + token + biometría + localización geográfica + perfil de usuario

- Modelos de control de acceso.-

Control de acceso obligatorio (MAC): en este modelo es el sistema quién protege los recursos, donde la autorización para que un sujeto acceda a un objeto depende de los niveles de seguridad que posee. Este modelo MAC se emplea habitualmente en el entorno militar.

Control de acceso discrecional (DAC): El modelo DAC se ha empleado comúnmente en sistemas operativos de propósito general, en todos los sistemas de bases de datos y sistemas de comunicaciones de propósito comercial. En este modelo el propietario del recurso, decide cómo protegerlo estableciendo cómo compartirlo, mediante controles de acceso impuestos por el sistema. El propietario del recurso puede cederlo a un tercero. Los modelos DAC y MAC son inadecuados para cubrir las necesidades de la mayor parte de las organizaciones. El modelo DAC es demasiado débil para controlar el acceso a los recursos de información de forma efectiva, en tanto que el MAC es demasiado rígido.

Control de acceso basado en roles (RBAC): En este modelo a los usuarios le son asignados uno o varios roles mientras que los permisos y privilegios se asignan a estos roles. Así las políticas de control de accesos basado en roles controlan el acceso de los usuarios a la información basándose en sus actividades y funciones de trabajo. Este modelo permite la construcción jerárquica de estas políticas de acceso, por tanto se reduce la complejidad y el coste de la administración de seguridad en entornos empresariales.

Contraseñas: Se refiere al grupo delimitado de caracteres que conforman una palabra secreta que sirve a un usuario con el fin de acceder a un determinado servicio o recurso. Las contraseñas generalmente están delimitadas en sus caracteres y su longitud (21).

Políticas de Contraseñas: establece las reglas de longitud, tipo de caracteres, nomenclatura de contraseñas de autenticación de usuario en red, las que se utilizan para determinar si una contraseña nueva es válida. Una regla de intensidad de contraseñas es una regla que una contraseña debe cumplir.

Empresa: organización compuesta por personal, máquinas, edificios, ingreso de materia prima, salida de productos, recursos económicos monetarios, objetivos institucionales y otros relacionados (22).

El Control de acceso a red: Está referido a los medios para manejar el acceso de usuarios a determinadas zonas de una red organizacional, incluyendo procedimientos, lineamientos, prácticas o estructuras organizacionales, destinados a la protección de la información contenida en la red o fuera de

ella; es el medio que ayuda a proteger, determinando que privilegios tiene un usuario en la red y a que recursos tendrá acceso, realizando restricción de la cantidad de usuarios, procesos y resguardar la información de accesos no autorizados (23).

2.2.4.2. Servidores

Son computadoras centrales en un sistema de red que proveen servicios a otras computadoras. Los clásicos servidores son de base de datos, de archivos, de correo, de impresión, servidor web, servidor de juegos, servidor de aplicaciones, servidor proxy y otros (24).

- Servidores Linux:

Son equipos hardware los cuales soportan el sistema operativo Linux para ambiente servidores, en sus diversas distribuciones bajo la licencia GNU, pueden brindar servicios de aplicaciones desarrollados bajo licencia de código abierto, servicios de correo, de archivos, ftp y otros; son altamente estables y robustos, cuentan con una comunidad variada de desarrolladores que ofrecen actualizaciones y soportes en línea. Son ideales para pequeñas y grandes empresas que dependen totalmente de la estabilidad de sus servicios.

- Servidores Windows:

Son equipos dedicados que ejecutan el sistema operativo Windows para servidores. Estos equipos alojan diversos sistemas de información, aplicaciones y otros; son recomendados a quienes mantengan proyectos bajo entorno

.ASP o .NET que requiera aplicar esta tecnología; sus costos de licenciamiento son mayores ya que la mayoría de las aplicaciones son de pago.

Sistema Operativo Windows Server: Es un sistema operativo diseñado para servidores de la línea Microsoft y varios tipos de productos enfocados al mercado de negocios. Así tenemos distintas versiones que han ido evolucionado con el tiempo como Windows server 2003, 2008, 2012, 2014, 2016 (25).

Sistemas Operativos clientes: Se refiere al software que controla la computadora de usuarios y hace uso de servicios suministrados por los servidores, así también controla la ejecución de otros programas compatibles (24).

Active Directory: Es la implementación de servicio de directorio en una red distribuida de computadores del fabricante Microsoft. Es un servicio escalable que permite administrar eficientemente los recursos de red ayudando a monitorizar y localizar estos servicios; funciona mediante la distribución de unidades organizativas en el que se pueden ubicar los recursos. Usa protocolos como LDAP, DNS, DHCP y Kerberos (25).

Unidades organizacionales: Es un tipo de objeto de directorio que se ubica en un dominio. Las unidades organizativas OU son contenedores de Active Directory donde se pueden colocar usuarios, grupos, equipos y otros.

Escritorio remoto: es un modo de administrar el servidor desde cualquier equipo de la red sin requerir licencia para este tipo de

conexión, permitiendo visualizar como una ventana en el escritorio local del cliente que está conectado al servidor (25).

Samba: es una implementación del protocolo de archivos compartidos de Windows para sistemas de tipo UNIX. Ello posibilita que computadoras con GNU/Linux, Mac o Unix se vean como servidores o actúen como clientes en redes de Windows. Samba permite validar usuarios haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; también permite servir como cola de impresión, directorios compartidos y autenticar con su propio archivo de usuarios (26).

Postfix: es un servidor de correo de código abierto que viene instalado en las distribuciones Linux, este programa informático permite el enrutamiento y envío de correo electrónico, creado con la intención de que sea una alternativa rápida y segura (26).

2.2.4.3. Seguridad.

La información: Se define como un fenómeno que proporciona significado o sentido a las cosas, e indica mediante códigos y conjuntos de datos, los modelos del pensamiento humano. La información procesa y genera el conocimiento humano a diferencia de los datos que son cifras y hechos crudos, sin analizar. En resumen la información es el resultado de haber organizado o analizado los datos de alguna manera y con un propósito (24).

Activo: es cualquier elemento o información, tenga o no valor contable para la organización (23).

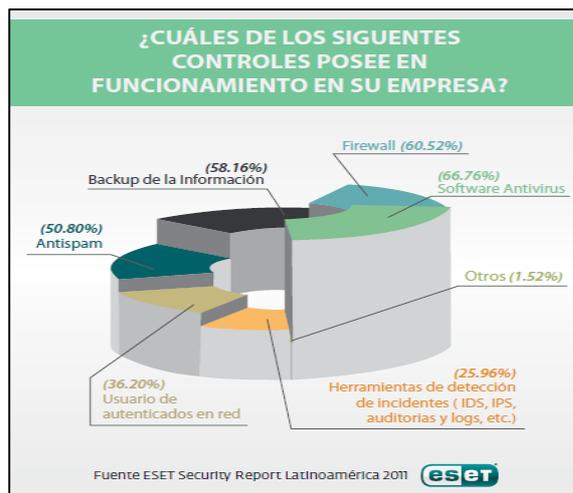
Confidencialidad: La información tiene que estar disponible y no sea divulgada a personas, entidades o procesos no autorizados (23).

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas (27).

Riesgo: Es la combinación de la probabilidad de un evento y su ocurrencia (23).

Controles de seguridad: La seguridad se consigue implantando un conjunto de políticas, procedimientos y funciones de software. Estos controles deberían establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la organización tratamiento del riesgo (28).

Gráfico Nro. 5: Controles de seguridad

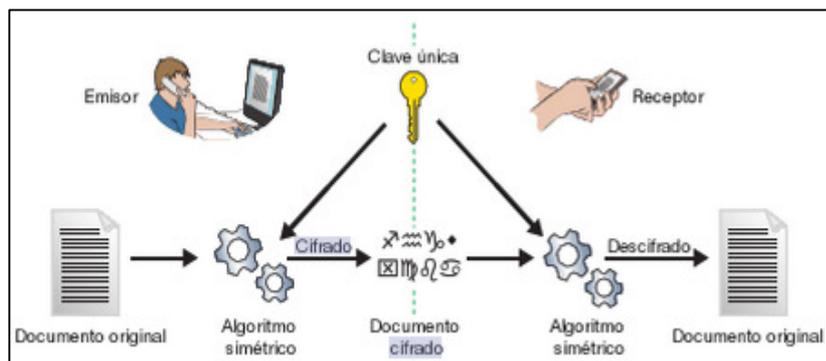


Fuente: ESET (28).

Cifrado: El cifrado es una medida de seguridad utilizada para proteger los datos alojados en un dispositivo. Consiste en alterar la información de acuerdo a un patrón establecido por una clave o llave, de modo que solamente puedan ser comprendidos por los que conocen esa clave.

Criptografía: consiste en aplicar un algoritmo a un documento original dando como resultado un nuevo documento cifrado, ininteligible al leerlo directamente, para luego hacerlo llegar a su destino donde se aplica el algoritmo para recuperar el documento original (29).

Gráfico Nro. 6: La criptografía



Fuente: Roa J. (29).

Aislamiento: este aspecto, íntimamente relacionado con la Confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.

La Prevención: mecanismos que aumentan la seguridad de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.

La Detección: mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

Intruso o Atacante: es la persona que accede o intenta acceder sin autorización a un sistema ajeno, ya sea en forma intencional o no. Clase A: son los nuevos intrusos que bajan programas de Internet y prueban. Clase B: son más peligrosos, saben compilar programas aunque no saben programar. Clase C: personas que saben, definen sus objetivos, luego buscan los accesos remotos e intentan ingresar. Clase D: son los que entran y buscan la información que necesitan (30).

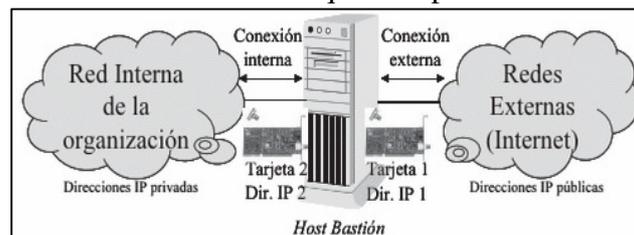
Gráfico Nro. 7: Triangulo de la intrusión



Fuente: Gómez Á. (31).

Firewall: es un sistema que se coloca entre dos redes y ejerce la política de seguridad establecida en la organización con el fin de proteger una red confiable de otra que no lo es. Existen dispositivos hardware de fabricantes conocidos que traen incorporado toda la lógica para esa función. Se puede configurar usando distribuciones especializadas (30).

Gráfico Nro. 8: Esquema típico de firewall



Fuente: Gómez Á. (31).

Estándares de la Seguridad de la Información: en el Perú se empezó a reglamentar las instituciones públicas con la norma NTP-ISO/OEC 27001:2005, luego se actualizó a NTP-ISO/IEC 27001:2008, NTP-ISO/IEC 27001:2013 y posteriormente a la NTP-ISO/IEC 2007:2014 (2).

Seguridad de los sistemas de información: Debido a que se almacenan grandes cantidades de datos en forma electrónica, éstos son vulnerables a muchos tipos de amenazas a las que no están expuestos los datos asentados en papel. Kennet Laudon (32), clasifica las amenazas más comunes que enfrentan los sistemas de información computarizados de la siguiente manera: fallos de hardware, fallos de software, acciones de personal, penetración por terminales, robos de datos, servicios, equipo, incendio, problemas eléctricos, errores de usuario, cambios de programa, problemas de telecomunicaciones.

Sistemas Biométricos: Es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas; la forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por manos, ojos, huellas digitales y voz (23).

Técnicas Biométricas: Están basadas en los siguientes indicadores biométricos: rostro, termograma del rostro, huellas dactilares, geometría de la mano, venas de las manos, Iris, patrones de la retina, voz.

Tipos de sistemas biométricos más usados: Lectores de Huellas Dactilares, son herramienta muy útil para restringir accesos y controlar el uso de dispositivos y áreas en instalaciones. Control Biométrico por Verificación de Voz, puede ser utilizado como medio de identificación. Biometría por Patrones Oculares, el iris y la retina pueden ser utilizados como medios de identificación en las personas, los controles biométricos basados en estos son muy efectivos, al igual que con las huellas dactilares, es casi imposible que alguien duplique o falsifique estas partes de nuestro cuerpo, haciéndolos altamente confiables. Emisión de calor, se utilizan en especial para identificar la presencia de personas en ciertas zonas, se facilita con el uso de cámaras especializadas para este fin.

Seguridad Lógica: es la implementación de límites y estándares que resguarden el acceso a los datos y sólo se permita acceder a quienes estén autorizados. Son mecanismos por software para proteger un sistema informático y la información que contiene, por ejemplo mediante el uso de contraseñas, encriptación de la información, antivirus, cortafuegos y otros (30).

Seguridad activa: Se refiere a un grupo de medidas que se emplean con el fin de detectar las amenazas, y en caso que sean detectadas generar los mecanismos adecuados para evitar el problema (29).

Seguridad pasiva: Se refiere a un grupo de medidas empleadas para que luego que se produzca el ataque o fallo, hacer que el impacto sea lo menor posible y luego activar procesos de recuperación (29).

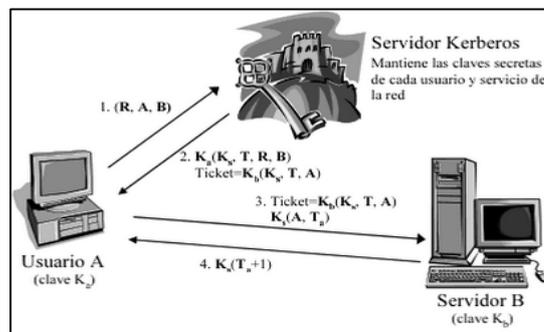
Seguridad física: Son mecanismos tangibles empleados en los equipos informáticos con el fin de proteger un sistema informático y la información contenida, por ejemplo haciendo uso de cámaras de seguridad, control de acceso al edificio y demás (29).

Amenazas: Todo aquello, físico o lógico, que puede provocar una pérdida de información, o su privacidad, o bien un fallo en los equipos físicos.

Mecanismos de seguridad: Son las denominadas barreras de seguridad. Son usadas para evitar o minimizar el efecto de las amenazas.

Kerberos: es un protocolo que permite autenticar redes de computadoras creado por el MIT en el cual dos computadoras en una red insegura pueden identificarse mutuamente de manera segura. Es muy usado en redes con servicio Active Directory. Usa la criptografía de clave simétrica para suministrar autenticación altamente segura entre cliente y servidor de aplicación, opera en base a "tickets" que se conceden por un tercero llamado centro de distribución de claves o KDC (31).

Gráfico Nro. 9: Sistema Kerberos



Fuente: Gómez Á. (31).

Autenticación: Es la verificación de la identidad de una persona, usuario o proceso, con el fin de tener acceso a determinados recursos o realizar ciertas tareas (23).

Gráfico Nro. 10: Esquema autenticación



Fuente: Colobran M., Arqués J. y Marco E. (23).

2.2.4.4. Entornos de desarrollo.

Ingeniería de Software.

Ciclo de vida.

Tabla Nro. 8: Ciclo de vida de software

Planificación	Desarrollo	Mantenimiento
Efectúa inventario de las actividades que se realizan en una empresa, se agrupan por proyectos que tengan una interrelación, se	Permite llevar a cabo las tareas que posibiliten el funcionamiento del proyecto. Incluye varias actividades como: análisis, diseño,	Persigue el objetivo de obtener una nueva versión de un sistema debido a peticiones de cambio sea por problema detectado, o por la

define el hardware, la topología de red, el lenguaje de programación, y se asigna prioridad a cada proyecto.	construcción, pruebas e implantación.	necesidad de mejora del mismo, las que no estuvieron plasmadas en la fase de definición.
--	---------------------------------------	--

Fuente: Sommerville I. (33).

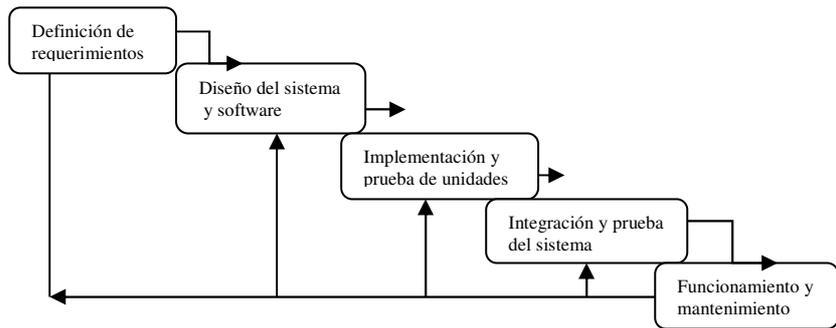
Comprende el mantenimiento: Correctivo, que involucra cambiar el software para corregir los defectos. Evolutivo, que sirve para introducir mejoras en el software. Adaptativo, en la cual se modifica el software para acomodarlo a los cambios de su entorno externo. Perfectivo, posibilita plasmar un software más allá de sus requisitos funcionales originales.

Modelos de procesos del software.-

Modelo en cascada o lineal secuencial:

Es la ejecución secuencial de una serie de fases en secuencia. Cada fase genera documentación para la siguiente, la que debe ser aprobada. Requiere definir los requisitos completos y precisos al principio del desarrollo.

Gráfico Nro. 11: Modelo cascada



Fuente: Sommerville I. (33).

Tabla Nro. 9: Modelo cascada

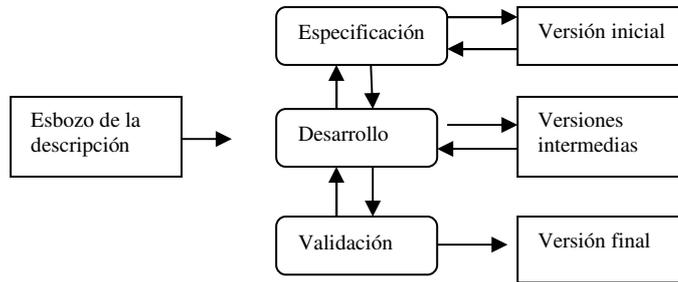
Ventajas	Desventajas
Facilita la gestión del desarrollo de software.	<ul style="list-style-type: none"> -Los requisitos no se pueden congelar mientras dura el desarrollo; -El cliente debe esperar mucho tiempo hasta ver los resultados; -Los errores de análisis y diseño son costosos de eliminar -Se genera mucho mantenimiento inicial y el código fuente se va deteriorando.

Fuente: Sommerville I. (33).

Modelo Desarrollo evolutivo:

Desarrolla una implementación inicial para comentarios del cliente.

Gráfico Nro. 12: Desarrollo evolutivo



Fuente: Sommerville I. (33).

Es ventajoso para sistemas pequeños y de tamaño medio.
Para sistemas grandes se recomienda un proceso mixto.

Modelo basado en componentes.

Presenta las etapas:

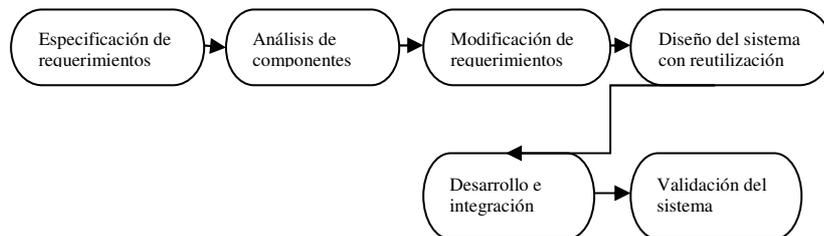
Análisis de componentes.

Modificación de requerimientos.

Diseño del sistema con reutilización.

Desarrollo e integración.

Gráfico Nro. 13: Modelo Basado en componentes



Fuente: Sommerville I. (33).

Metodologías de desarrollo del software.

Proporcionan cobertura total del ciclo de vida del desarrollo, son flexibles, permiten una fácil formación y están soportadas por herramientas automatizadas, son personalizables, presentan interfaces con procesos de gestión,

Clasificación:

- Estructuradas.
- Orientadas a procesos.
- Orientadas a datos.
- Para el desarrollo de sistemas de tiempo real.
- Orientadas a objetos.
- Formales.
- Mixtas

Metodologías oficiales:

Merise.- Considera tres niveles de abstracción:

- Nivel conceptual: define el qué.
- Nivel organizativo: Define la organización a implantar para alcanzar los objetivos.
- Nivel físico: Se ocupa de los medios técnicos.

SSADM.- Cubre las fases:

- Estudio de viabilidad.
- Estudio completo: Análisis de requisitos.
- Diseño físico.

Métrica v3.- Tiene como objetivos, Mantener la sencillez, flexibilidad y adaptabilidad. Estructura: Proceso principal: Descripción general.

Proceso: Descripción general y productos generados.

Actividad: Descripción y tareas de que consta. Productos generados por la actividad, técnicas utilizadas y participantes

Tarea: Descripción, productos de entrada y de salida, técnicas y participantes.

Métodos ágiles.- Principios

Tabla Nro. 10: Métodos ágiles

Participación del cliente	Proporcionar nuevos requerimientos del sistema
Entrega incremental	Se desarrolla en incrementos
Personas no procesos	Explotar las habilidades del equipo.
Aceptar el cambio	Dar cabida a los cambios
Simplicidad	Eliminar la complejidad

Fuente: Sommerville I. (33).

Programación extrema.- Principios

Tabla Nro. 11: Programación extrema

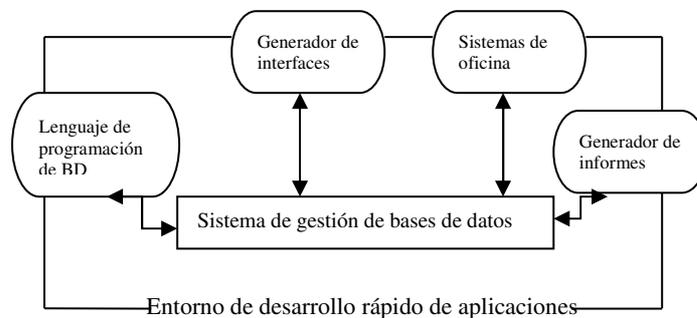
Desarrollo incremental se lleva en entrega pequeñas.	Basado en historias del cliente
Participación del cliente a tiempo completo.	Participan en el desarrollo y aceptación de las pruebas.
Programación en parejas.	Evitar jornadas excesivas.
Entrega regulares.	Integración continua.
Refactorización constante.	Mejorar la calidad del código.

Fuente: Sommerville I. (33).

Desarrollo rápido de aplicaciones RAD.- Herramientas:

- Lenguaje de programación de bases de datos: SQL
- Generador de interfaces, para crear los formularios
- Enlaces a aplicaciones de oficina, hoja de cálculo y procesador de textos.
- Generador de informes.

Gráfico Nro. 14: RAD

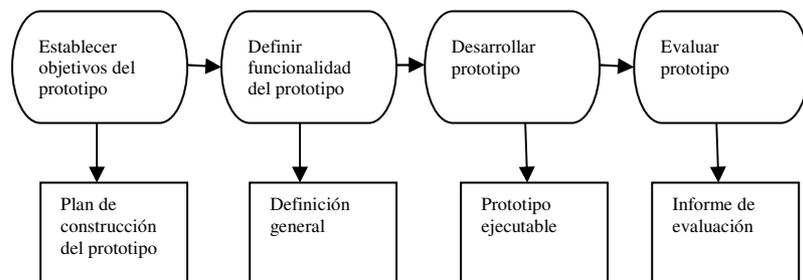


Fuente: Sommerville I. (33).

El desarrollo visual es un enfoque a RAD, tal como el Visual Basic.

Prototipado del software.-

Gráfico Nro. 15: Proceso desarrollo



Fuente: Sommerville I. (33).

Metodología SCRUM:

Es un marco de trabajo para la gestión y desarrollo de software basada en un proceso incremental. SCRUM estaba enfocado a la gestión de procesos de desarrollo de software, puede ser utilizado en equipos de mantenimiento de software, o en una aproximación de gestión de programas.

Programación extrema:

Más conocido como eXtreme Programming (XP) es una metodología de desarrollo de la ingeniería de software formulada por Kent Beck. Pone más énfasis en la adaptabilidad que en la previsibilidad, se basa en la simplicidad, la comunicación y el reciclado continuo de código.

Gile Unified Process:

El proceso unificado ágil de Scott Ambler o agile unified process (AUP) es una versión simplificada del proceso unificado de rational (RUP). AUP aplica técnicas ágiles incluyendo desarrollo dirigido por pruebas (test driven development - TDD), modelado ágil, gestión de cambios ágil, y refactorización de base de datos para mejorar la productividad.

UML.-

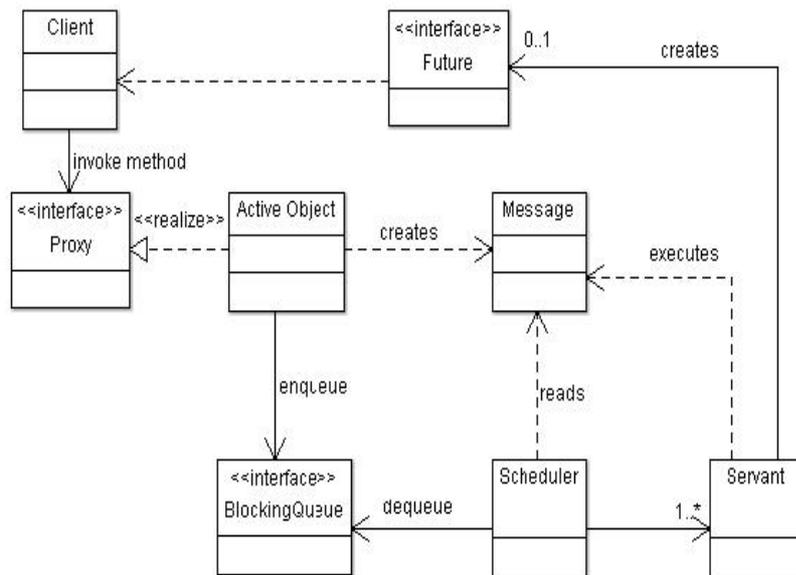
Es una notación orientada a objetos, el cual se compone de diferentes diagramas, los cuales representan las diferentes etapas del desarrollo del proyecto. Es un tipo de diagrama de estructura estática que describe la estructura de un sistema

mostrando las clases del sistema. Fue creado para mostrar modelado visual común y rico para la arquitectura, el diseño y la implementación de sistemas de software complejos. UML tiene aplicaciones más allá del desarrollo de software, como en el flujo de procesos en la fabricación.

Los fines de UML son:

Brindar a los desarrolladores de software las herramientas para el análisis, el diseño y la implementación de sistemas basados en software, así como para el modelado de procesos de negocios y similares. No obstante, para habilitar un intercambio significativo de información de modelos entre herramientas, se requiere de un acuerdo con respecto a la semántica y notación.

Gráfico Nro. 16: Ejemplo diagrama UML



Fuente: Sommerville I. (33).

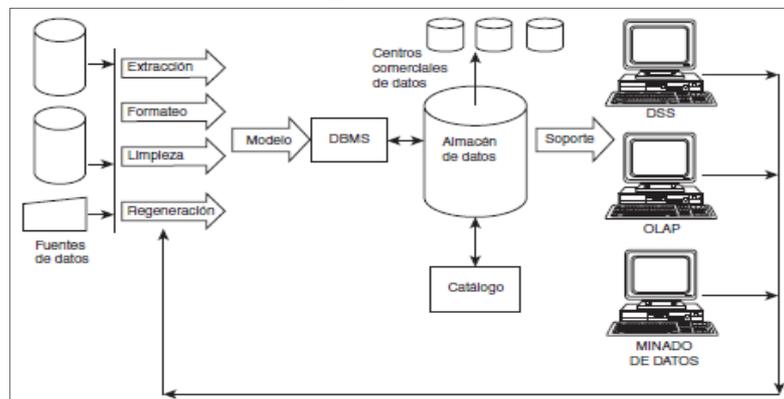
Plataforma: es una integración de servidores y herramientas que posibilita implementar soluciones que pueden ser de escritorio, web, ftp, otros, incluida aplicaciones y servidores auxiliares (34).

Plataforma de desarrollo: es el entorno de software común en el cual se desenvuelve la programación de un grupo de aplicaciones.

Diagrama de clases: es un tipo de diagrama de estructura que permite visualizar la estructura de un sistema mostrando las clases del sistema, sus atributos, métodos y las relaciones entre los objetos.

Bases de datos: Es un repositorio organizado que representa algunos aspectos del mundo real elegidos por el programador. Así la base de datos SQL tiene un lenguaje de definición de datos completos y lenguaje de manipulación de datos; las operaciones tienen lugar en un marco temporal llamado transacción, estas transacciones se inician con BEGIN TRANS, a continuación se resuelven mediante una validación (35).

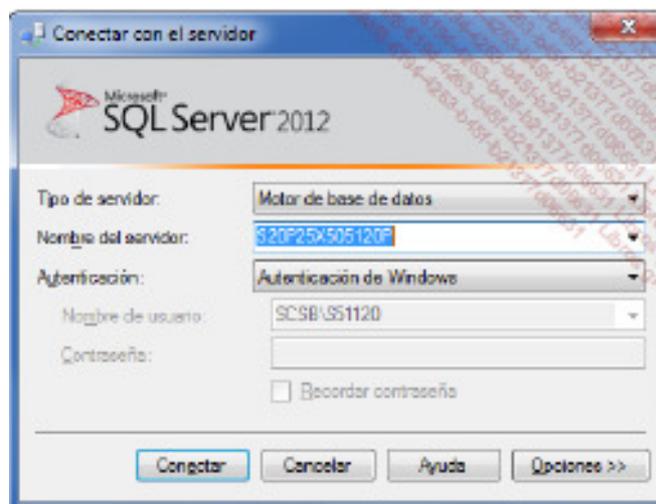
Gráfico Nro. 17: Arquitectura de bases de datos



Fuente: Catherine R. (35).

SQL Server: es un sistema de gestión de base de datos que usa lenguaje de consulta relacional SQL estándar. A nivel lógico, cada relación se representa mediante una tabla base. A nivel externo consiste en vistas, que se generan a partir de subconjuntos, combinaciones u otras relaciones en las tablas base (35).

Gráfico Nro. 18: SQL server



Fuente: Catherine R. (35).

Entorno de Desarrollo Integrado IDE: Se denomina así al entorno de programación que soporta diversas actividades relacionadas al desarrollo de aplicaciones, tales como la creación de interfaces gráficas, la inclusión asistida de código fuente o incluso pruebas unitarias. Para ello incorpora un editor de código, un compilador, un depurador y un constructor de interfaz gráfica (GUI) (36).

Lenguaje de programación: Se refiere al lenguaje artificial que es usado para controlar el comportamiento de una máquina o computadora. Siguen reglas sintácticas y semánticas que permiten expresar instrucciones que luego serán interpretadas.

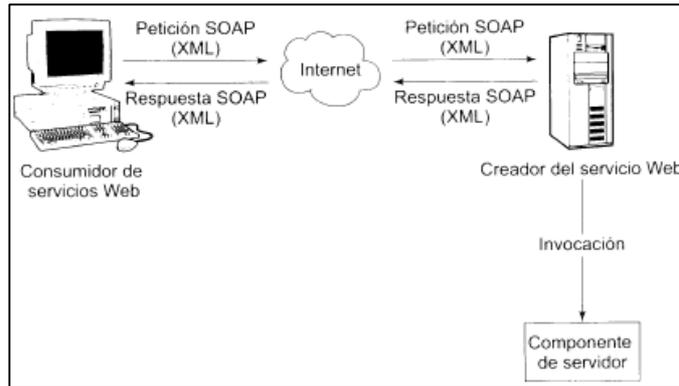
Se clasifican en procedimentales, orientado a objetos, funcionales, lógicos y otros (21).

Visual Studio: Pertenece a la familia de entornos de desarrollo integrado IDE; es una plataforma de desarrollo del fabricante Microsoft que presenta las versiones Visual Studio profesional, Express y Visual Studio Web Developer Express. Los productos soportan el modo WYSIWYG y aseguran la parte esencial del proceso de desarrollo de aplicaciones .NET y ASP.NET (36).

Netbeans: es un entorno de desarrollo integrado realizado especialmente para el lenguaje de programación Java. Esta hecho en base a módulos que permite extender su desempeño; es un producto libre y gratuito sin restricciones de uso y bajo licencia GNU. Tiene éxito en base a la colaboración de una comunidad de usuarios en constante crecimiento. Fue la empresa Sun Microsystems quien fundó el proyecto de código abierto Netbeans en junio de 2000 y continúa siendo el patrocinador principal.

Lenguaje C#: es un lenguaje de programación sencillo, amigable y poderoso. Con C# se pueden crear todo tipo de aplicaciones, desde programas de consola para Windows con páginas web en unión con ASP, hasta video juegos para Xbox 360 con XNA (37).

Gráfico Nro. 19: Programación C#



Fuente: Landa N. (37).

WPF (Windows Presentation Foundation): Es una tecnología de Microsoft que permite diseñar y generar aplicaciones de escritorio y de forma atractiva. Incluye características de aplicaciones web, permite diseñar interfaz gráfica por medio del formato XAML, así como aplicar estilos tal como se hace en el entorno web con CSS y aplicar el patrón de arquitectura MVC. Internamente utiliza la API Direct3D, por ello se puede crear aplicaciones muy atractivas, con movimientos dinámicos, interactuar con animaciones, vídeo, audio, documentos, aplicar efectos.

III. HIPÓTESIS

3.1. Hipótesis General

La implementación del sistema de control de acceso a red en la empresa SIMA - Chimbote, mejora el control de cuentas de usuarios y la seguridad de la red.

3.2. Hipótesis específicas

1. La evaluación tecnológica de la plataforma de servidores Linux, Windows y computadoras clientes, permite establecer los requisitos mínimos de hardware y software para el adecuado diseño del sistema de control de acceso de usuarios a red.
2. La evaluación de las configuraciones existentes en los servidores Active Directory, Linux y Windows, permite establecer el alcance y limitaciones del sistema propuesto, a fin no alterar el funcionamiento de los sistemas de información desarrollados en la empresa.
3. La evaluación del entorno de desarrollo más conveniente a utilizar, permite mayores prestaciones en la codificación del sistema de control de acceso.
4. El control manual de las cuentas de usuarios y el peligro por suplantación en la red generan la necesidad de desarrollar la propuesta de implementar un sistema de control de acceso a red.

IV. METODOLOGÍA

4.1. Diseño de la investigación

La investigación se basó en el diseño No experimental y por las características de su ejecución fue de Corte Transversal.

La investigación fue no experimental porque se realizó sin manipular deliberadamente variables ya que se observaron los hechos tal como se dieron en su contexto natural, para luego ser analizados; y de corte transversal porque se recolectaron datos en una fecha determinada, en un momento único (38).

4.2. Población y Muestra

La población estuvo conformada por 10 usuarios, quienes interactúan permanentemente con esta actividad y laboran en la división de tecnologías de la información DTIC. La muestra seleccionada fueron los 10 usuarios de esta división. Luego se aplicó la recolección de datos al personal seleccionado, para obtener una adecuada y especializada información.

La población se refiere al conjunto de todos los casos que concuerdan con determinadas especificaciones, pueden ser grupos sociales con características comunes, grupos laborales, grupo de empresas y otros (38).

En esta investigación se utilizó el método no probabilístico, con muestra por conveniencia. Se eligió este modo teniendo en cuenta a quienes interactúan permanentemente con esta actividad, además que no todo el personal usuario de la red de servicios informáticos estaba en igualdad de condiciones de ser elegido para muestra, por estar destacado en actividades fuera de la empresa o encontrarse de vacaciones.

La muestra se refiere a una parte de la población en estudio, la cual se elige para ahorrar tiempo y recursos, lo cual conlleva a definir unidad de muestreo y análisis, así también delimitar la cantidad a fin de proyectar los resultados. Existen las clases probabilística, en el cual se define el tamaño de la muestra; y no probabilística por conveniencia, en la cual no toda la población está en igualdad de condiciones de ser elegido para muestra (38).

Tabla Nro. 12: Resumen de población y muestra

Grupo	Población	Muestra
Usuarios DTIC	10	10

Fuente: Elaboración propia.

4.3. Definición operacional de las variables en estudio

Tabla Nro. 13: Matriz de operacionalización de la variable Implementación de un Sistema de Control de acceso a red.

Variable	Definición conceptual	Dimensiones	Indicadores	Escala de medición	Definición operacional
Implementación de un Sistema de control de acceso a red.	La implementación es la etapa en el cual se escribe el código del programa y se construye el prototipo para registrar y depurar el funcionamiento (24).	Nivel de satisfacción con respecto al actual esquema de control de acceso a red.	<ul style="list-style-type: none"> - Satisfacción con la atención brindada. - Compartir recursos de la PC asignada. - Acceso a puertos USB. - Instalación de software por el usuario en la PC asignada. - Acceso a internet sin restricciones. - Políticas de acceso a internet. - Cambio de contraseña de usuario luego de una reasignación de puesto. - Cancelación de privilegios en todos los servidores a los usuarios que dejan de laborar en la empresa. - Registro de los incidentes relacionados con accesos a red. - Uso de herramientas y/o configuraciones para identificar automáticamente a los equipos que se conectan a la red. 	Ordinal	<ul style="list-style-type: none"> • SI • NO

	<p>Sistema de control de acceso a red se refiere a al proceso que posibilita el acceso a datos o recursos en un entorno corporativo luego de la autenticación (39).</p>	<p>Necesidad de propuesta para el control de acceso por medio de un sistema.</p>	<ul style="list-style-type: none"> - La implementación de un sistema de control mejorará el control de accesos de usuarios a red. - El sistema propuesto debe ser amigable de usar para el administrador. - Hay funciones que deben incorporarse en el sistema de control propuesto. - El actual proceso de control de accesos debe mejorar. - El sistema propuesto debe incorporar funciones centralizadas en mayor medida. - El sistema propuesto debe considerar reportes fáciles de acceder y permitir que el Jefe TI haga seguimiento. - La implementación del nuevo sistema dará mayor funcionalidad y seguridad. - Debe mejorarse la eficiencia en el control de accesos. - El sistema propuesto debe permitir que el mismo usuario cambie periódicamente su contraseña de acceso a red de acuerdo a las políticas. - El sistema debe incluir aviso al usuario vía correo antes de la caducidad de la contraseña de red. 		
--	---	--	---	--	--

Fuente: Elaboración propia.

4.4. Técnicas e instrumentos de recolección de datos.

4.4.1. Técnica

Las técnicas en esta investigación fueron:

Encuesta: que es una técnica de recolección de información por medio de preguntas organizadas en un cuestionario impreso. En este caso se elaboró cuestionario para la encuesta respectiva según se indica en el anexo 03. Se basó en las dimensiones: satisfacción actual por atención de cuentas de acceso y necesidad de implementar un sistema de control de acceso a red.

Revisión documentaria: comprendió la investigación de material bibliográfico tales como normas técnicas peruanas e internacionales, informe de tesis de grado, libros digitales, manuales, revistas científicas y lectura de registros de seguimiento de averías de la empresa.

4.4.2. Instrumentos.

El instrumento que se utilizó fue:

Cuestionario: es un documento específico que permite al analista recoger la información y las opiniones que manifiestan las personas que los responden.

El instrumento elaborado fue consultado directamente a los usuarios del área DTIC de la empresa, constaba de preguntas con dos alternativas de respuesta, a fin de conocer temas relacionados al control de acceso a red.

4.5. Plan de análisis

Los datos obtenidos fueron codificados y luego ingresados en hoja de cálculo del programa Microsoft Excel 2013. Además se procedió a la tabulación de los mismos. Se realizó el análisis de datos que sirvió para establecer las frecuencias y realizar el análisis de distribución de dichas frecuencias.

4.6. Matriz de consistencia

Tabla Nro. 14: Matriz de consistencia

Problema	Objetivo general	Hipótesis general	Variables	Metodología
Implementación de un sistema de control de acceso a red.	Realizar la Implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote, con el fin de mejorar el control de las cuentas de usuarios y la seguridad de la red.	La implementación del sistema de control de acceso a red en la empresa SIMA - Chimbote, mejora el control de cuentas de usuarios y la seguridad de la red.	Implementación de un sistema de control de acceso a red.	Enfoque Cuantitativo.
	Objetivos específicos	Hipótesis específicas		Investigación Descriptiva.
	1. Realizar una evaluación tecnológica de la plataforma de servidores Linux y Windows que brindan los servicios informáticos, incluido la plataforma de computadoras clientes.	1. La evaluación tecnológica de la plataforma de servidores Linux, Windows y computadoras clientes, permite establecer los requisitos mínimos de hardware y software para el adecuado diseño del sistema de control de acceso de usuarios a red.		Diseño No experimental.
				Corte Transversal.

	<p>2. Realizar una evaluación de las configuraciones existentes en los servidores Active Directory, Linux y Windows, con el fin de establecer el alcance y limitaciones del sistema propuesto, para no alterar el funcionamiento de los Sistemas de Información desarrollados en la empresa.</p> <p>3. Realizar una evaluación del entorno de desarrollo más apropiado que permita la centralización e interacción del sistema de control de acceso a red con el servidor Active Directory, servidores Linux y servidores Windows.</p>	<p>2. La evaluación de las configuraciones existentes en los servidores Active Directory, Linux y Windows, permite establecer el alcance y limitaciones del sistema propuesto, a fin no alterar el funcionamiento de los sistemas de información desarrollados en la empresa.</p> <p>3. La evaluación del entorno de desarrollo más conveniente, permite mayores prestaciones en la codificación del propuesto sistema de control de acceso a red.</p>		
--	--	--	--	--

	4. Desarrollar la propuesta de diseño del sistema de control de acceso a red en la empresa SIMA - Chimbote, 2018, con el fin mejorar el control de las cuentas de usuarios y la seguridad de la red.	4. El control manual de las cuentas de usuarios y el peligro por suplantación en la red generan la necesidad de desarrollar la propuesta de implementar un sistema de control de acceso a red.		
--	--	--	--	--

Fuente: Elaboración propia.

4.7. Principios éticos

Durante el desarrollo de la presente investigación denominada Implementación de un Sistema de control de Acceso a Red en la Empresa SIMA - Chimbote; 2018, se consideró en forma estricta el cumplimiento de los principios éticos que permitan asegurar la originalidad de la Investigación. Asimismo, se respetó los derechos de propiedad intelectual de los libros de texto y de las fuentes electrónicas consultadas, necesarias para estructurar el marco teórico.

Por otro lado, considerando que gran parte de los datos utilizados son de carácter público, y pueden ser conocidos y empleados por diversos analistas sin mayores restricciones, se ha incluido su contenido sin modificaciones, salvo aquellas necesarias por la aplicación de la metodología para el análisis requerido en esta investigación.

Igualmente, se conserva intacto el contenido de las respuestas, manifestaciones y opiniones recibidas de los trabajadores y funcionarios que han colaborado contestando las encuestas a efectos de establecer la relación causa-efecto de la o de las variables de investigación. Finalmente, se ha creído conveniente mantener en reserva la identidad de los mismos con la finalidad de lograr objetividad en los resultados.

V. RESULTADOS

5.1. Resultados

5.1.1. Dimensión 1: Nivel de satisfacción actual.

Tabla Nro. 15: Satisfacción por la atención de cuentas de acceso.

Respuestas acerca del nivel de satisfacción actual en relación a la satisfacción por la atención de cuentas de acceso; con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	3	30.00
No	7	70.00
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Se siente satisfecho por la atención referente a sus cuentas de acceso?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 15 se puede observar que el 70% respondió que NO está satisfecho con la atención referente a sus cuentas de acceso, en tanto que el 30% de usuarios encuestados respondió que SI está satisfecho con la atención referente a sus cuentas de acceso.

Tabla Nro. 16: Compartir recursos de la PC.

Respuestas acerca del nivel de satisfacción actual en relación a compartir recursos de la PC; con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	5	50.00
No	5	50.00
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Puede compartir recursos de la PC asignada?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 16 se puede observar que el 50% de usuarios encuestados respondió que SI puede compartir recursos de la PC asignada, en tanto que el 50% respondió que NO puede compartir recursos de la PC asignada.

Tabla Nro. 17: Acceso a puertos USB.

Respuestas acerca del nivel de satisfacción actual en relación al acceso a puertos USB; con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	3	30.00
No	7	70.00
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Tiene acceso a puertos USB?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 17 se puede observar que el 70% respondió que NO tiene acceso a puertos USB, en tanto que el 30% de usuarios encuestados respondió que SI tiene acceso a puertos USB.

Tabla Nro. 18: Instalar software en la PC asignada.

Respuestas acerca del nivel de satisfacción actual en relación a la instalación de software en la PC; con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	1	10.00
No	9	90.00
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Puede instalar software en la PC asignada?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 18 se puede observar que el 90% respondió que NO puede instalar software en su PC, en tanto que el 10% de usuarios encuestados respondió que SI puede instalar software en su PC.

Tabla Nro. 19: Acceso a internet sin restricciones.

Respuestas acerca del nivel de satisfacción actual en relación al acceso a internet sin restricciones; con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	2	20.00
No	8	80.00
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Hay acceso a internet sin restricciones?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 19 se puede observar que el 80% respondió que NO hay acceso a internet sin restricciones, en tanto que el 20% de usuarios encuestados respondió que SI hay acceso a internet sin restricciones.

Tabla Nro. 20: Políticas de acceso a internet.

Respuestas acerca del nivel de satisfacción actual en relación a las políticas de acceso a internet; con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	6	60.00
No	4	40.00
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿existen políticas de acceso a internet?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 20 se puede observar que el 60% de usuarios encuestados respondió que SI existen políticas de acceso a internet, en tanto que el 40% respondió que NO existen políticas de acceso a internet.

Tabla Nro. 21: Cambio de contraseña luego de una reasignación.

Respuestas acerca del nivel de satisfacción actual en relación al cambio de contraseña luego de reasignación de puesto; con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	8	80.00
No	2	20.00
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Se cambia la contraseña de usuario luego de una reasignación de puesto?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 21 se puede observar que el 80% de usuarios encuestados respondió que SI se realiza el cambio de la contraseña de usuario luego de una reasignación de puesto, en tanto que el 20% respondió que NO se realiza el cambio de la contraseña de usuario luego de una reasignación de puesto.

Tabla Nro. 22: Cancelación de privilegios.

Respuestas acerca del nivel de satisfacción actual en relación a la cancelación de privilegios en los servidores a los usuarios que dejan de laborar; con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Se realiza la cancelación de privilegios en todos los servidores a los usuarios que dejan de laborar en la empresa?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 22 se puede observar que el 100% de usuarios encuestados respondió que SI se realiza la cancelación de privilegios en todos los servidores cuando los usuarios dejan de laborar, en tanto que se registró 0% con la alternativa NO.

Tabla Nro. 23: Registro de los incidentes de la red.

Respuestas acerca del nivel de satisfacción actual en relación al registro de incidentes; con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	5	50.00
No	5	50.00
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Se registran los incidentes relacionados con accesos a red?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 23 se puede observar que el 50% de usuarios encuestados respondió que SI se registran los incidentes relacionados con accesos a red, en tanto que el 50% respondió que NO se registran los incidentes relacionados con accesos a red.

Tabla Nro. 24: Identificar a los equipos que se conectan a la red.

Respuestas acerca del nivel de satisfacción actual en relación a las herramientas de detección automática de equipos en red; con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	4	40.00
No	6	60.00
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Se tiene herramientas y/o configuraciones para identificar automáticamente a los equipos que se conectan a la red?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 24 se puede observar que el 60% respondió que NO se tiene herramientas para identificar automáticamente a los equipos que se conectan a la red, en tanto que el 40% de usuarios encuestados respondió que SI se tiene herramientas para identificar automáticamente a los equipos que se conectan a la red.

Tabla Nro. 25: Resumen dimensión 1 Nivel de satisfacción.

Alternativas	n	%
Si	5	50.00
No	5	50.00
Total	10	100.00

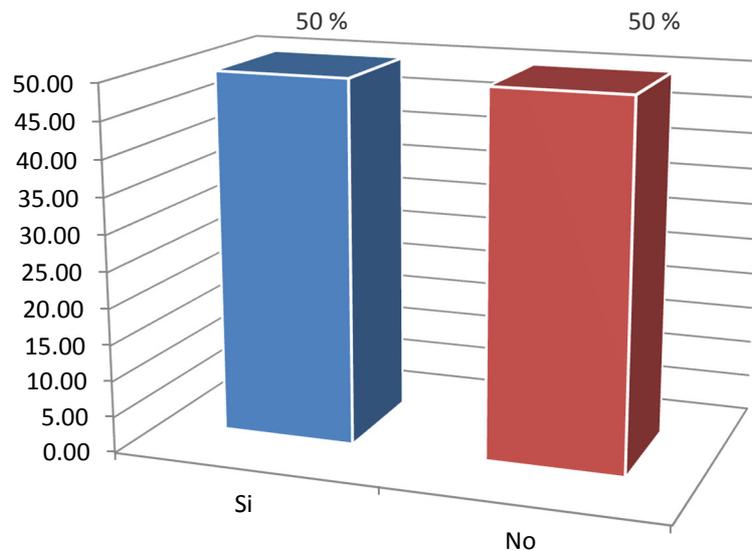
Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, con relación a la dimensión 1.

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 25 se muestra el resumen de la dimensión 1 donde se puede notar que un 50% de usuarios encuestados respondió que SI está satisfecho por la atención de sus cuentas de acceso a red, en tanto que el restante 50% respondió que NO está satisfecho por la atención de sus cuentas de acceso a red.

Gráfico Nro. 20: Resumen Dimensión 1

Resumen acerca de la dimensión nivel de satisfacción actual por la atención de cuentas de acceso; con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.



Fuente: Tabla Nro. 25.

En el Gráfico Nro. 20 se muestra el resumen de la dimensión 1 donde se puede observar que un 50% de usuarios encuestados respondió que SI está satisfecho por la atención de sus cuentas de acceso a red, en tanto que el restante 50% respondió que NO está satisfecho por la atención de sus cuentas de acceso a red.

5.1.2. Dimensión 2: Necesidad de implementación.

Tabla Nro. 26: Mejora de control de accesos de usuarios.

Respuestas acerca de la necesidad de implementación en relación a la mejora en el control de acceso; con referencia al propuesto sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Cree que la implementación de un sistema de control mejorará el control de accesos de usuarios a red?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 26 se puede observar que el 100% de usuarios encuestados respondió que la implementación de un sistema de control SI mejorará el control de accesos de usuarios a red, en tanto que se registró 0% con la alternativa NO.

Tabla Nro. 27: Sistema propuesto amigable de usar.

Respuestas acerca de la necesidad de implementación en relación a la interfaz del sistema propuesto; con referencia al propuesto sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Cree que es necesario que el sistema propuesto sea amigable de usar para el administrador y permita procesar las tareas en menor tiempo?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 27 se puede observar que el 100% de usuarios encuestados respondió que SI es necesario que el sistema propuesto sea amigable de usar, en tanto que se registró 0% con la alternativa NO.

Tabla Nro. 28: Incorporar funciones en el sistema propuesto.

Respuestas acerca de la necesidad de implementación en relación a incorporar funciones; con referencia al propuesto sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Cree usted que hay funciones que requieren incorporarse en el sistema de control propuesto?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 28 se puede observar que el 100% de usuarios encuestados respondió que SI es necesario que el sistema propuesto incorpore funciones, en tanto que se registró 0% con la alternativa NO.

Tabla Nro. 29: Mejorar el actual proceso de control de accesos.

Respuestas acerca de la necesidad de implementación en relación a mejorar el actual proceso de control; con referencia al propuesto sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Cree que el actual proceso de control de accesos debe mejorar?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 29 se puede observar que el 100% de usuarios encuestados respondió que SI se debe mejorar el actual proceso de control de accesos en tanto que se registró 0% con la alternativa NO.

Tabla Nro. 30: Implementar funciones centralizadas.

Respuestas acerca de la necesidad de incorporar funciones centralizadas; con referencia al propuesto sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Es necesario que el sistema propuesto considere funciones centralizadas en mayor medida que los actuales?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 30 se puede observar que el 100% de usuarios encuestados respondió que SI es necesario que el sistema propuesto considere funciones centralizadas en mayor medida que los actuales, en tanto que se registró 0% con la alternativa NO.

Tabla Nro. 31: Reportes ágiles que permitan supervisión.

Respuestas acerca de la necesidad de considerar reportes ágiles en la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Cree que es necesario que el sistema propuesto considere reportes ágiles, fáciles de acceder y posibiliten que el Jefe TI haga seguimiento?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 31 se puede observar que el 100% de usuarios encuestados respondió que SI es necesario que el sistema propuesto considere reportes ágiles que posibiliten la supervisión, en tanto que se registró 0% con la alternativa NO.

Tabla Nro. 32: Funcionalidad y seguridad.

Respuestas acerca de la necesidad de la propuesta que permita mayor funcionalidad y seguridad, con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Cree que la implementación del nuevo sistema dará mayor funcionalidad y seguridad en el control de accesos a red?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 32 se puede observar que el 100% de usuarios encuestados respondió que la implementación del nuevo sistema SI dará mayor funcionalidad y seguridad en el control de accesos a red, en tanto que se registró 0% con la alternativa NO.

Tabla Nro. 33: Eficiencia en el control de accesos.

Respuestas acerca de la necesidad de implementación para mejorar la eficiencia; con referencia al sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	8	80.00
No	2	20.00
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Cree que debe mejorarse la eficiencia del control de accesos?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 33 se puede observar que el 80% de usuarios encuestados respondió que SI debe mejorarse la eficiencia del control de accesos a red, en tanto el 20% respondió que NO debe mejorarse la eficiencia.

Tabla Nro. 34: Permitir que el mismo usuario cambie su contraseña.

Respuestas acerca de la necesidad de implementación que permita que el mismo usuario cambie su contraseña; con referencia al sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	8	80.00
No	2	20.00
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Cree que el sistema propuesto debe permitir que el mismo usuario cambie periódicamente su contraseña de acceso a red de acuerdo a las políticas de la empresa?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 34 se puede observar que el 80% de usuarios encuestados respondió que el sistema propuesto SI debe permitir que el mismo usuario cambie periódicamente su contraseña, en tanto que el 20% respondió que NO debe permitir el cambio periódico de contraseña por el mismo usuario.

Tabla Nro. 35: Notificación vía correo por caducidad de contraseña.

Respuestas acerca de la necesidad de implementación en relación a notificación por correo antes de caducidad de contraseña; con referencia al sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, en relación a la pregunta: ¿Cree que el usuario debe ser notificado vía correo con antelación a la caducidad de su contraseña de red?

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 35 se puede observar que el 100% de usuarios encuestados respondió que SI se debe notificar vía correo al usuario antes de la caducidad de su contraseña, en tanto se registró 0% con la alternativa NO.

Tabla Nro. 36: Resumen dimensión 2: necesidad de implementación

Alternativas	n	%
Si	10	100.00
No	-	-
Total	10	100.00

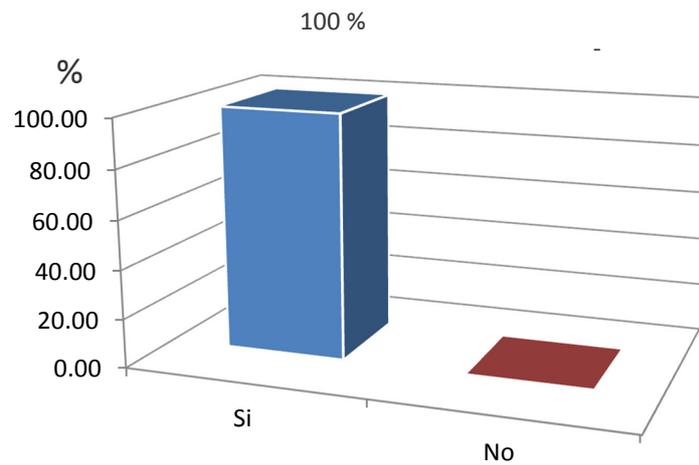
Fuente: Origen del instrumento aplicado a los usuarios del área División de Tecnologías de la Información y Comunicaciones del SIMA - Chimbote, con relación a la dimensión 2.

Aplicado por: Martinez, J.; 2018.

En la Tabla Nro. 36 se muestra el resumen de la dimensión 2 donde se puede notar que un 100% de usuarios encuestados respondió que SI es necesario la implementación de un sistema de control de acceso a red, en tanto que se registró 0% con la alternativa NO.

Gráfico Nro. 21: Resumen Dimensión 2

Resumen acerca de la dimensión, necesidad de implementación, con referencia a la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.



Fuente: Tabla Nro. 36.

En el Gráfico Nro. 21 se muestra el resumen de la dimensión 2 donde se puede observar que el 100% de usuarios encuestados respondió que SI es necesario la implementación de un sistema de control de accesos a red, en tanto se registró 0% con la alternativa NO.

5.2. Análisis de resultados

Este trabajo de investigación estuvo orientado a realizar la implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote, con el fin de mejorar el control de las cuentas de usuarios y la seguridad de la red; por lo cual se tuvo que aplicar el instrumento de recojo de información para analizar la percepción de los usuarios de la división de tecnologías de la información y comunicaciones del SIMA - Chimbote frente a las dos dimensiones que se propusieron en esta investigación. Por ello, a partir de la interpretación de los resultados mostrados en la sección anterior se realizó los siguientes análisis:

- En relación a la dimensión 1: nivel de satisfacción del actual control de acceso a red, se evidencia que un 50% de usuarios encuestados respondió que SI está satisfecho con la atención de sus cuentas de acceso a red, en tanto que el restante 50% respondió que NO está satisfecho con la atención de sus cuentas de acceso a red, este resultado indica que hay un porcentaje significativo de usuarios que no están satisfechos con el estado actual de la atención de cuentas de acceso y por lo cual se tiene que mejorar; ello tiene relación con el trabajo de los autores Zuñiga M. y Guevara L. (11), quienes en su tesis “Diseño e implementación de un sistema en plataforma Web y Android para control de acceso en la empresa minera Antapaccay” mostraron que hubo mejoras significativas con la implementación de un sistema de control de acceso en dicha organización; asimismo tiene relación con lo expresado por el autor Roa J. (29), en su libro “Seguridad Informática” quien establece que hay mejoras ostensibles en materia de seguridad al usar mecanismos de control donde cada usuario tenga su contraseña (con caducidad), que permita en cualquier momento añadir o eliminar usuarios, así también llevar un registro de quién entra a la red en cada momento.

- En relación a la dimensión 2: necesidad de implementación de un sistema de control de acceso a red, se puede apreciar que el 100% de usuarios encuestados respondió que SI se necesita la implementación, a su vez se registró 0% de respuestas con la alternativa NO, este resultado plantea la necesidad de implementar mejoras a través de un sistema de control de acceso; ello está en relación con los resultados obtenidos por Blas J. (8), quien en su tesis “Seguridad y control del acceso a las redes inalámbricas en la UNSM-T mediante servidores de autenticación Radius con el uso de Certificados Digitales” planteó la necesidad de implementar sistemas de control con el fin de mejorar la seguridad en su organización; de igual modo está en concordancia con los lineamientos expuestos en la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 (2), que plantea con carácter imperativo la implementación de un control de usuarios, haciendo uso de sistemas de control adecuados a fin de prevenir accesos no autorizados a los servicios de red.

De lo expuesto se concluye que la implementación de un sistema de control de acceso a red en la empresa SIMA – Chimbote mejora el control de cuentas de usuarios y la seguridad de la red.

5.3. Propuesta de mejora

Evaluación de la plataforma tecnológica

Para tener adecuado desarrollo del sistema se evaluó la plataforma de sistemas operativos servidores y clientes de la red, teniendo en cuenta el criterio siguiente: presencia de lista de control de acceso, compatibilidad con sistema de control, versión de framework.

Tabla Nro. 37: Sistema operativo servidores en SIMA - Chimbote

Servidor	Sistema operativo	Presenta lista de control de acceso	Compatibilidad con Sistema de control
Active Directory	Windows Server 2008 R2	Si	Si
Controlador de Dominio	Windows Server 2008 R2	Si	Si
Base de Datos	Windows Server 2008 R2	Si	Si
Web	Windows Server 2008 R2	Si	Si
Aplicaciones	Linux CentOS	Si	Si
Correo	Linux CentOS	Si	Si

Fuente: SIMA – Chimbote (15).

Tabla Nro. 38: Sistemas Operativos Clientes en SIMA - Chimbote

Estaciones Clientes	Sistema operativo	Cantidad	Versión Framework	Compatibilidad con sistema de control
	Windows XP	107	4.0	Si
Windows Vista	10	4.0	Si	
Windows 7	151	4.5	Si	
Windows 8	1	4.5	Si	

Fuente: SIMA – Chimbote (15).

Evaluación de configuraciones existentes en servidores.

La empresa SIMA – Chimbote presenta un entorno de red compuesta por enlace backbone de fibra óptica, cableado UTP cat6, equipos switch core, switch de distribución y switch de borde, los cuales en conjunto conforman una red segmentada controlada por Active Directory y con VLAN. Criterio: compatibilidad con sistema de control.

Tabla Nro. 39: Configuraciones existentes

Servidor	Configuraciones de servicios y políticas	Compatibilidad con sistema de control
Active Directory	GPO control de puertos USB, CD/DVD,	No
	Grupos de acceso a internet por niveles.	Si
	GPO control de cuenta administrador.	Si
	GPO restricción de instalación de software.	No
	GPO protector de pantalla.	No
Aplicaciones	Servicio Samba: bloqueo de redes foráneas.	Si
	Servicio Samba: restricción de acceso a unidades de red F, G, H, solo lectura, lectura/escritura.	No
	Servicio Samba: bloqueo de extensiones de archivos.	No
	Cuotas de almacenamiento por usuario.	No
	Servicio de correo Postfix con filtro de contenido por	No

Correo	amavis: antivirus, antispam.	
	Integración con servicio de correo Exchange del SIMA – Callao.	No

Fuente: SIMA – Chimbote (15).

Evaluación de entornos de desarrollo integrado más comunes.

Se eligió desarrollar la propuesta del sistema de control usando un entorno de desarrollo integrado IDE de acuerdo a los siguientes criterios: curva de aprendizaje baja, permitir creación de proyectos para visualizar de forma gráfica, integrar herramientas de rediseño, poseer navegador incorporado para pruebas, poseer soporte para diversos lenguajes de programación, permitir reconocimiento de sintaxis, permitir importar y exportar proyectos. A continuación se expone las tablas de evaluación requeridas.

Tabla Nro. 40: Evaluación IDE Netbeans

	Integración con Linux	Integración con Windows: Active Directory
IDE Netbeans 8	Sí se integra nativamente.	No se integra completamente con Active Directory.
	No es necesario instalaciones adicionales.	Requiere instalación de certificados digitales en el Active Directory.
	Desempeño transparente en Linux.	Requiere instalación de librería JNDI en Active Directory.

Fuente: Elaboración propia.

Tabla Nro. 41: Evaluación IDE Eclipse

	Integración con Linux	Integración con Windows: Active Directory
Eclipse	Sí se integra nativamente.	No se integra completamente con Active Directory.
	No es necesario instalaciones adicionales.	Requiere instalación de certificados digitales en el Active Directory.
	Requiere agregar varios plugins para que funcione al cien por ciento.	Requiere instalación de librería JNDI en Active Directory.

Fuente: Elaboración propia.

Tabla Nro. 42: Evaluación IDE Visual Studio .Net

	Integración con Linux	Integración con Windows: Active Directory
Visual Studio .Net	Total integración de las librerías de conectividad con sistemas Linux.	Total integración con Active Directory, a través de su clase: System.DirectoryServices
	Es ideal para aplicaciones de escritorio y entorno web.	Es ideal para aplicaciones de escritorio y entorno web.
	No necesita instalaciones adicionales en servidores.	Mejor desarrollo gráfico con la tecnología WPF y visual C#.

Fuente: Elaboración propia.

5.3.1. Requerimientos de implementación y desarrollo

Luego de lo presentado en la Tabla Nro. 37, Tabla Nro. 38, Tabla Nro. 39, Tabla Nro. 40, Tabla Nro. 41 y Tabla Nro. 42, se definió los siguientes requerimientos de implementación y desarrollo:

Tabla Nro. 43: Requerimientos implementación

RI01	Compatible con los sistemas operativos Windows XP, Vista, 7, 8.
RI02	Compatible con la versión .Net Framework 4.0 y posteriores, lo cual garantiza funcionalidad con el sistema operativo Windows XP
RI03	No instalar software adicional en los servidores en Active Directory, en servidor Linux de aplicaciones y en servidor Linux de correo.
RI04	Elegir el entorno de desarrollo Visual Studio .Net WPF con C#, por sus ventajas de integración con Active Directory y servidores Linux. Además porque se acopla a las características de nuestro proyecto, las cuales son las siguientes: - Se requiere de un sistema escritorio compatible con Active Directory y Linux. - Que se puedan detectar rápidamente los errores para su corrección oportuna.

Fuente: Elaboración propia

La propuesta de implementación del sistema de control de acceso consta de:

Módulo Gestión de Usuarios:

- Administrar usuarios.
- Desplegar Formulario para cambiar contraseñas de usuarios.

- Eliminar usuarios en servidores AD y Linux.

Módulo Gestión de PC:

- Reubicar entre áreas.
- Reasignar.
- Eliminar de Active Directory

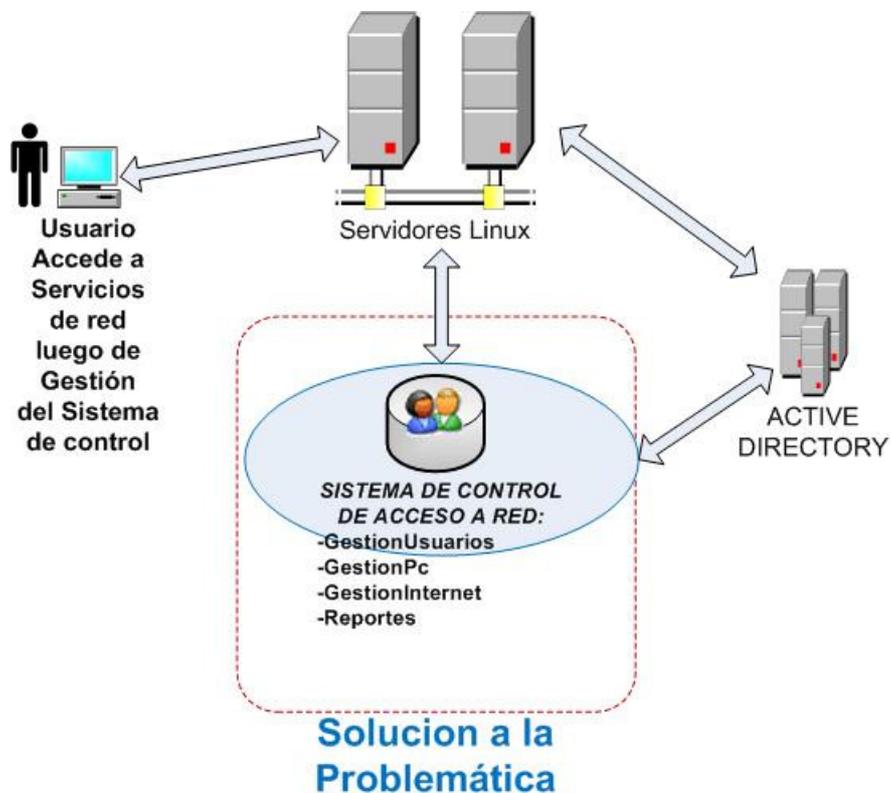
Módulo Gestión Acceso a Internet:

- Asignar nivel de acceso a internet.
- Bloquear acceso a internet

Módulo Reportes:

- Reportar requerimientos.
- Reportar por usuarios.
- Reportar por áreas.
- Reportar por Sistema operativo de PC.
- Los reportes deben permitir exportarse a Pdf, hoja de cálculo.

Gráfico Nro. 22: Esquema del sistema



Fuente: Elaboración propia.

Tabla Nro. 44: Actividades de Control de acceso a red.

1. Gestión de usuarios	Formato/Documento Sima (memo + área + nrodoc)
1.1 Crear usuarios nuevos asignándoles cuenta de acceso en el Active Directory y en los servidores Linux, en base a su nombre y apellido, evitando la duplicidad.	Memorándum de la oficina de personal con el requerimiento del caso.
1.2 Asignar grupo organizacional y/o mover entre grupos en el Active Directory (AD).	Memorándum de la oficina de personal con el requerimiento del caso.
1.3 Eliminar usuarios de la red en AD y servidores Linux, según requerimiento.	Memorándum de la oficina de personal con requerimiento de baja.
1.4 Generar reportes con filtros.	Requerimiento de Jefatura DTIC.
2. Gestión de PC	Formato/Documento Sima
2.1 Identificar las PC en el dominio según políticas de la empresa.	Memorándum de oficina de personal con requerimiento.
2.2 Mover entre áreas en Active Directory.	Memorándum de la oficina de personal con el requerimiento.
2.3 Generar Reportes de PC por sistema operativo, por áreas, etc.	Requerimiento de Jefatura DTIC.
3. Gestión Acceso a Internet	formato/documento
3.1 Agregar, mover usuarios de los niveles de acceso a internet.	Memorándum de jefe de área del usuario solicitante.
3.2 Deshabilitar acceso a internet	Memorándum de jefe de área del usuario solicitando la baja.
3.3 Reportar por áreas, por niveles.	Requerimiento de Jefatura DTIC.

Fuente: Elaboración propia.

5.3.2. Requerimientos funcionales

Tabla Nro. 45: Requerimientos funcionales.

Requerimientos Funcionales del Sistema	
RF01.- Ubicación de uso del aplicativo	<ul style="list-style-type: none"> - En el área División Tecnologías de Información del SIMA - Chimbote. - Disponible en servidor de aplicaciones.
RF02.- Zona Geográfica	<ul style="list-style-type: none"> - Instalaciones del SIMA - Chimbote
RF03.- Responsabilidad	Según responsabilidades de los Actores del Negocio
RF04.- Flujos Operacionales Identificados	<ul style="list-style-type: none"> - Gestión de usuarios: Concierno las operaciones de creación, movimiento, baja. - Gestión de PC: Identificación, reasignación, movimiento. - Gestión acceso a Internet: asignación, movimiento. - Gestión de Reportes: reportes por usuarios, por áreas, por nivel de acceso, por sistema operativo.
RF05.- Importancia de las funciones del Sistema	<p>Priorizar las funciones del sistema de acuerdo a los siguientes aspectos:</p> <ul style="list-style-type: none"> - Atención al usuario y soporte. - Ejecución de Servicios. - Planificación y control.

<p>RF06.- Expectativas del nivel de servicio</p>	<ul style="list-style-type: none"> - Fácil de usar y de administrar - Información concisa y confiable. - Seguridad y acceso a la información. - Integración con tecnologías de comunicaciones y correo. - Disponibilidad de los servicios del sistema de 7.30am a 6:00pm
<p>RF07.- Expectativas Técnicas</p>	<ul style="list-style-type: none"> - Escalable, Arquitectura que permita implementar en el futuro nueva funcionalidades. - Autonomía del sistema, incluye la necesidad de adaptarse a los cambios organizacionales y realidades diferentes.

Fuente: Elaboración propia

5.3.3. Requerimientos no funcionales

Tabla Nro. 46: Requerimientos no funcionales.

Requerimientos no funcionales del sistema	
<p>RNF01.-Acceso y Seguridad</p>	<ul style="list-style-type: none"> - Los permisos de acceso al sistema solo podrán ser cambiados por el administrador o supervisor. - Seguridad integrada con los servicios de directorio. - Acceso directo a funciones de interés para PC de uso propio. - Acceso a través de servidor de aplicaciones desde un sitio único. - Respaldo del sistema cada 24 horas.

RNF02.- Implementación de Modelos de negocio	Las necesarias para atender a los modelos del negocio: - Procesos Según el “Diagrama de Procesos” - Usuarios Indicado en “Actores del negocio” - Casos de uso Indicado en “Casos de Uso”
RNF03.- Volumen de Datos (mensual)	- Soporte aproximado 30 requerimientos - Usuarios +/- 280
RNF04.- Usabilidad	- Tiempo de aprendizaje del sistema por un usuario menor a 4 horas. - Proporcionar mensajes de error que sean informativos y orientados a usuario final. - Poseer interfaces gráficas bien formadas. - Adecuada visualización en múltiples computadores personales.

Fuente: Elaboración propia.

Tabla Nro. 47: Requerimientos de hardware y software.

Requerimientos de hardware y software	
RT01.- Arquitectura	Distribuida, en red.
RT02.-Costos de la Red	Implementación en red existente.
RT03.- Requerimientos de Hardware	Compatible con equipos clientes, requerimiento mínimo Core2 Duo, procesador 3.0 GHz, 1 GB de RAM.

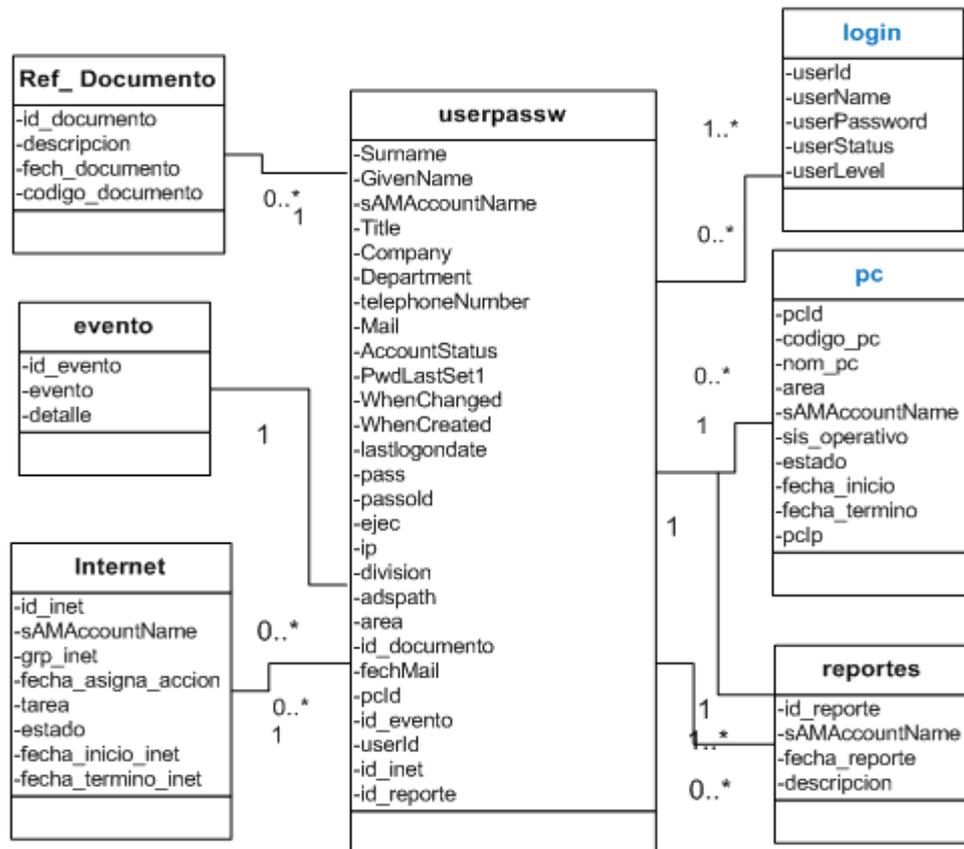
Requerimientos de hardware y software	
RT04.- Requerimientos mínimos de software	Ejecución compatible con sistemas operativos Windows xp, vista, 7, 8, 10, .Net Framework versión 4.0 o superior, resolución de pantalla 800 x 600, cliente de correo MS Outlook 2003 y Outlook Express 5.

Fuente: Elaboración propia.

Diagrama de clases.-

Para este trabajo se modeló el diagrama de clases en base a los requerimientos establecidos, ver el siguiente gráfico:

Gráfico Nro. 23: Diagrama de clases



Fuente: Elaboración propia.

Definición de Actores Primarios y secundarios.-

Tabla Nro. 48: Definición de actores.

Nombre	Primario	Secundario
Administrador	Si	
Supervisor	Si	
Usuario		Si
Base de datos		Si

Fuente: Elaboración propia.

Tabla Nro. 49: Actividades administrador

Nombre	Administrador.
Rol:	Acceder al sistema, configurar, gestionar.
Tipo:	Primario
Tareas:	Administrar el sistema, configurar los parámetros generales, crear usuarios, roles y permisos, gestionar las PC del dominio, gestionar acceso a internet, generar reportes.

Fuente: Elaboración propia.

Tabla Nro. 50: Actividades Supervisor.

Nombre	Supervisor.
Rol:	Acceder al sistema, auditoria de cambios.
Tipo:	Primario
Tareas:	Administrar el sistema, ver y/o solicitar reportes, gestionar las PC del dominio, gestionar acceso a internet.

Fuente: Elaboración propia.

Tabla Nro. 51: Actividades Usuario.

Nombre	Usuario.
Rol:	Cambiar su contraseña.
Tipo:	Secundario.
Tareas:	Usar el formulario de cambio de contraseña de acceso a la red, lo cual es replica a los servidores Linux de aplicaciones y de correo, según políticas de la empresa.

Fuente: Elaboración propia

Tabla Nro. 52: Actividades Base datos.

Nombre	Base de datos.
Rol:	Almacén principal de datos.
Tipo:	Secundario.
Tareas:	Representa a la base de datos del sistema, almacena datos de usuarios, roles, permisos, historiales de cambios, vigencia de contraseñas, gestión de PC, gestión de internet.

Fuente: Elaboración propia.

5.3.4. Casos de Uso

Tabla Nro. 53: Casos de uso

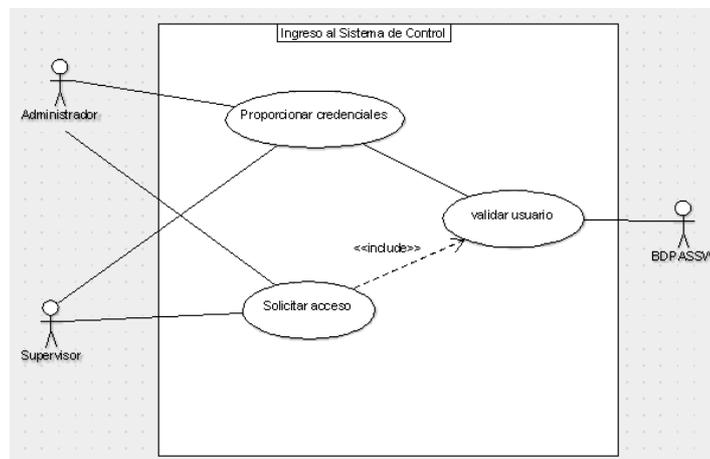
Código	Descripción
CU01	Ingresar al sistema
CU02	Requerimiento de creación de usuario
CU03	Crear usuario de red.
CU04	Asignar nivel de usuario.
CU05	Cambiar contraseña de acceso.
CU06	Verificar vigencia de contraseñas.
CU07	Controlar acceso a internet.
CU08	Generar reportes.
CU09	Generar Backup del sistema.

Fuente: Elaboración propia.

CU01 - Ingresar al sistema.

Se inicia cuando el administrador o supervisor requiere ingresar al sistema, para lo cual digita su cuenta “administrador” y “contraseña”. Se verifica que exista en el sistema, que la cuenta y contraseña digitadas sean correctos; de lo contrario muestra mensaje: “usuario o contraseña incorrectos”. Termina cuando el actor ingresa al sistema.

Gráfico Nro. 24: CU01 Ingresar al sistema.

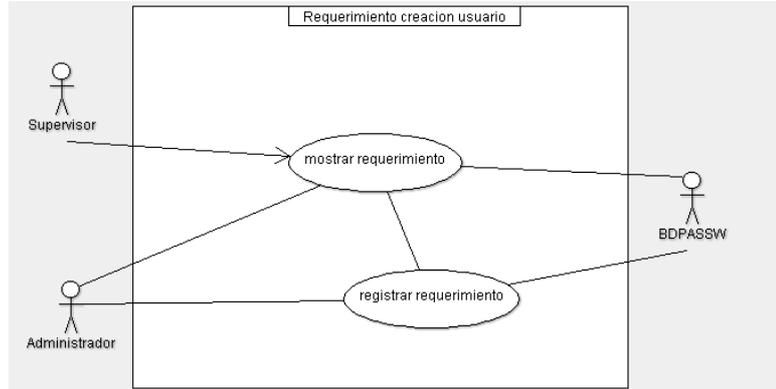


Fuente: Elaboración propia.

CU02 – Requerimiento Crear usuario.

Se inicia cuando el Administrador recibe requerimiento de creación de usuario por parte del Jefe TI, para ello registra el código, número de documento y detalle. El caso de uso termina cuando queda registrado el requerimiento.

Gráfico Nro. 25: CU02 Requerimiento crear usuario

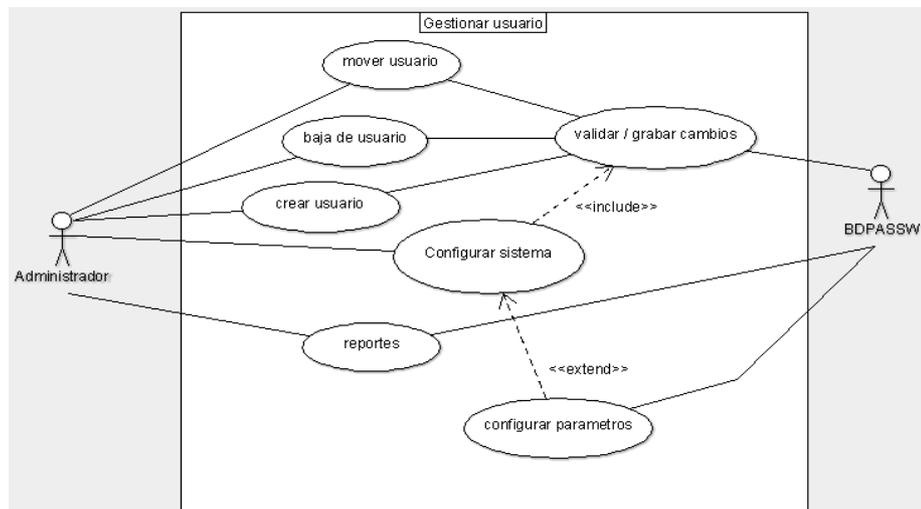


Fuente: Elaboración propia.

CU03 – Crear usuario de red.

Se inicia cuando el Administrador genera nueva cuenta de usuario, verifica que no existe en el sistema por lo cual procede a ingresar los datos del usuario detallados en el caso de uso CU02: nombres y apellidos, área de trabajo, descripción de funciones, contraseña inicial de acceso, cuenta de correo, nombre de pc asignada y documento de autorización, modificación de datos, movimiento entre áreas, dar de baja a la cuenta en el dominio, termina cuando se le asigna una cuenta al usuario.

Gráfico Nro. 26: CU03 Crear usuario de red.

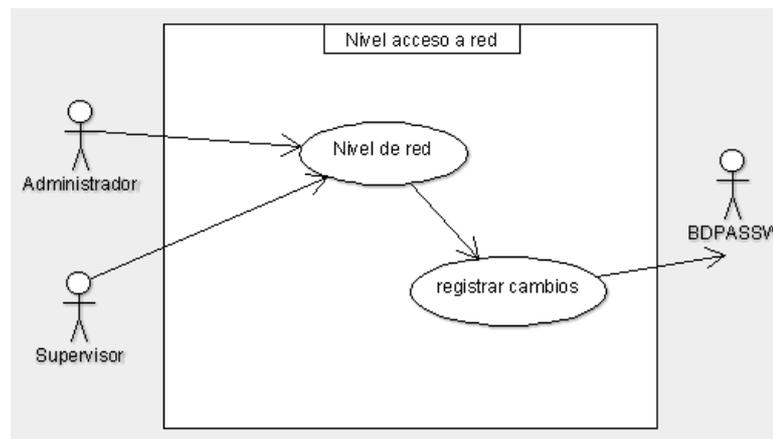


Fuente: Elaboración propia.

CU04 – Asignar nivel de usuario.

Se inicia cuando el administrador asigna nivel de acceso según sea jefe de área, analista, secretaria, en concordancia con el documento de requerimiento. Termina cuando el usuario verifica su acceso usando su nueva contraseña luego del cual queda registrado la actividad.

Gráfico Nro. 27: CU04 Nivel de usuario

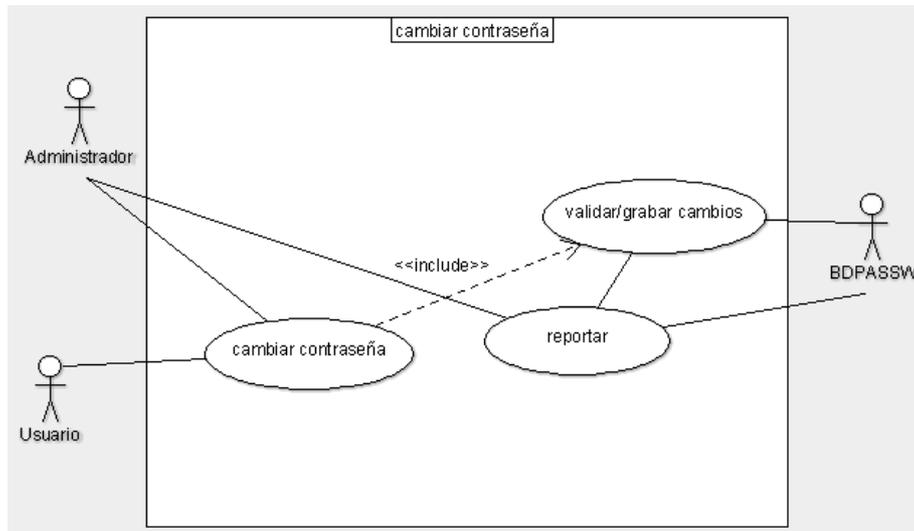


Fuente: Elaboración propia

CU05 – Cambiar contraseña de acceso a red.

Se inicia cuando el usuario procede a cambiar su contraseña haciendo uso del formulario respectivo y digita los datos requeridos (contraseña actual y contraseña nueva) acorde a la política de acceso de la empresa. El caso de uso termina cuando el usuario verifica su acceso usando su nueva contraseña luego del cual queda registrado la actividad.

Gráfico Nro. 28: CU05 Cambiar contraseña de acceso

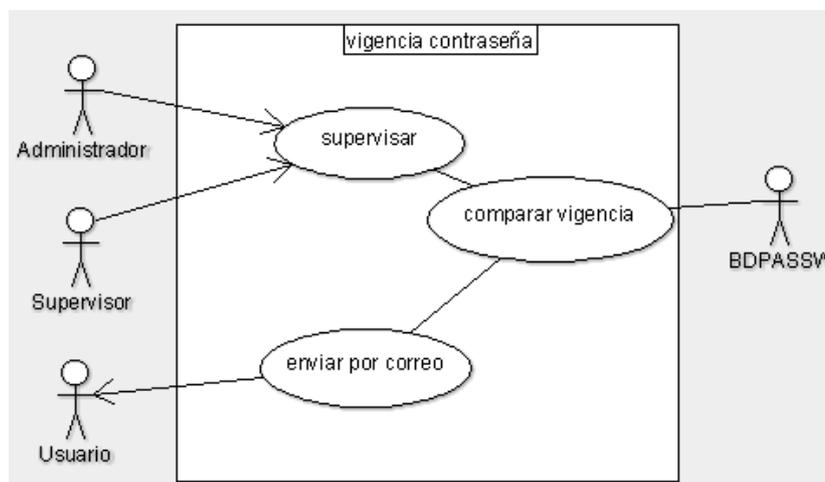


Fuente: Elaboración propia

CU06 – Verificar vigencia de contraseña.

Se inicia cuando el sistema detecta que la contraseña de un usuario ha superado los días de vigencia establecidos y emite notificación del vencimiento vía correo, a la vez que envía el link del aplicativo. El caso de uso termina cuando el usuario accede al aplicativo y procede a digitar su nueva contraseña.

Gráfico Nro. 29: CU06 Verificar vigencia de contraseña.

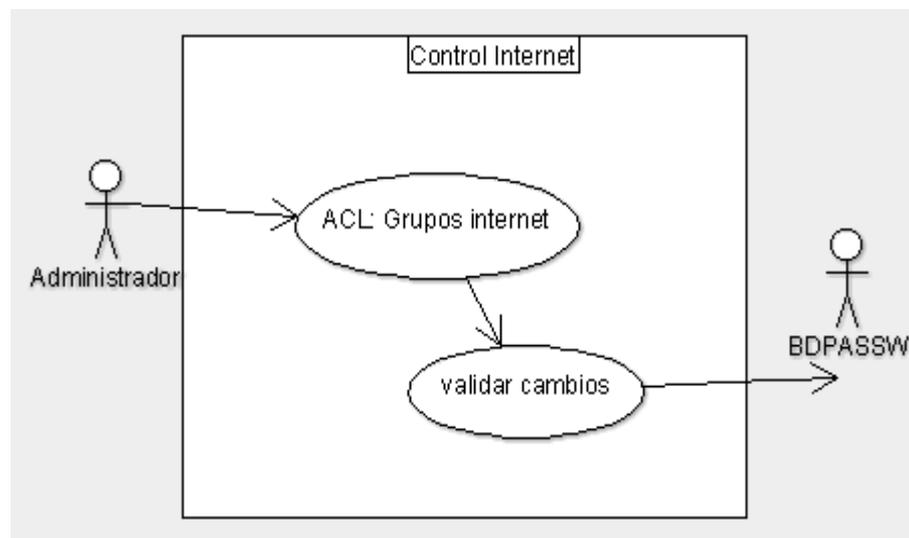


Fuente: Elaboración propia

CU07 – Controlar acceso a internet.

Se inicia cuando el administrador gestiona el acceso a internet para el usuario según lista ACL desplegadas en Active Directory, luego agrega el usuario al grupo respectivo según funciones descritas en el documento referencia. El caso de uso termina cuando el usuario verifica su acceso a internet.

Gráfico Nro. 30: CU07 Controlar acceso a internet

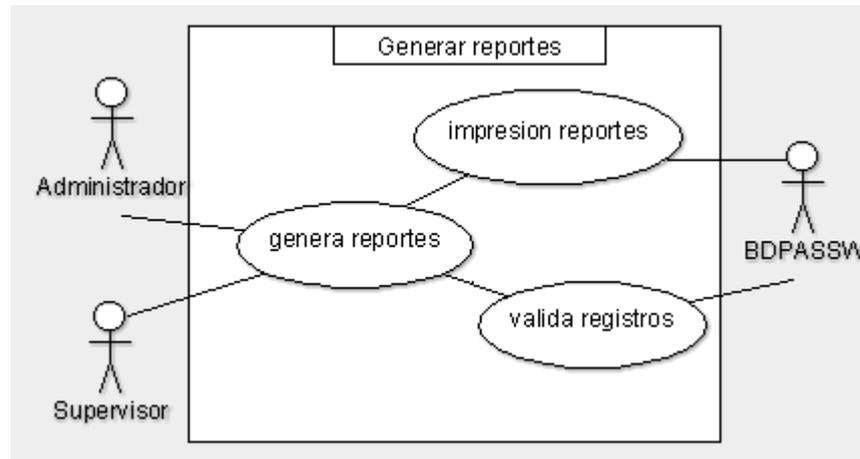


Fuente: Elaboración propia

CU08 – Generar reportes.

Se inicia cuando el administrador o supervisor generan reportes haciendo uso del módulo Reportes, según área, usuario, PC, otros, para ser impresos o almacenados en formato digital. Termina cuando se completa el reporte.

Gráfico Nro. 31: CU08 Generar reportes

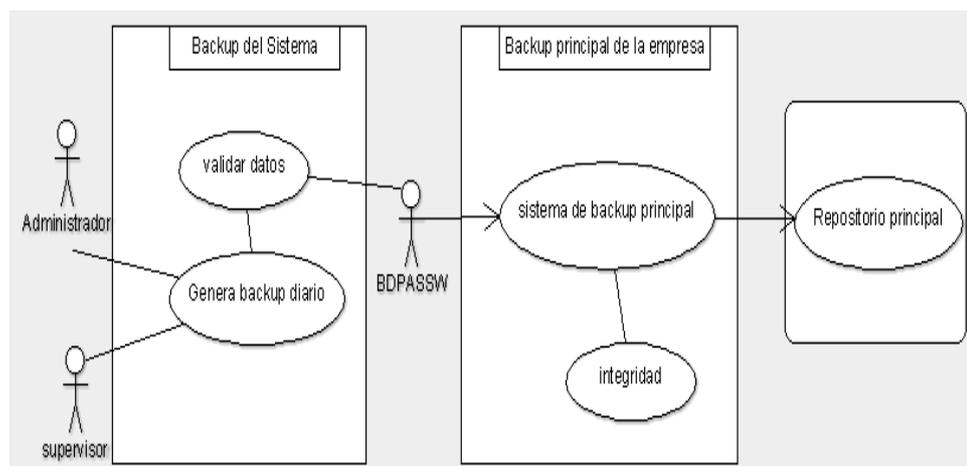


Fuente: Elaboración propia

CU09 – Generar Backup del sistema.

Inicia cuando el administrador o supervisor incluyen en el programa de backup diario de la empresa la copia de seguridad de la base de datos del sistema de control, la cual es revisada diariamente para comprobar su integridad. Termina cuando se localiza el backup en el repositorio principal de backup de la empresa.

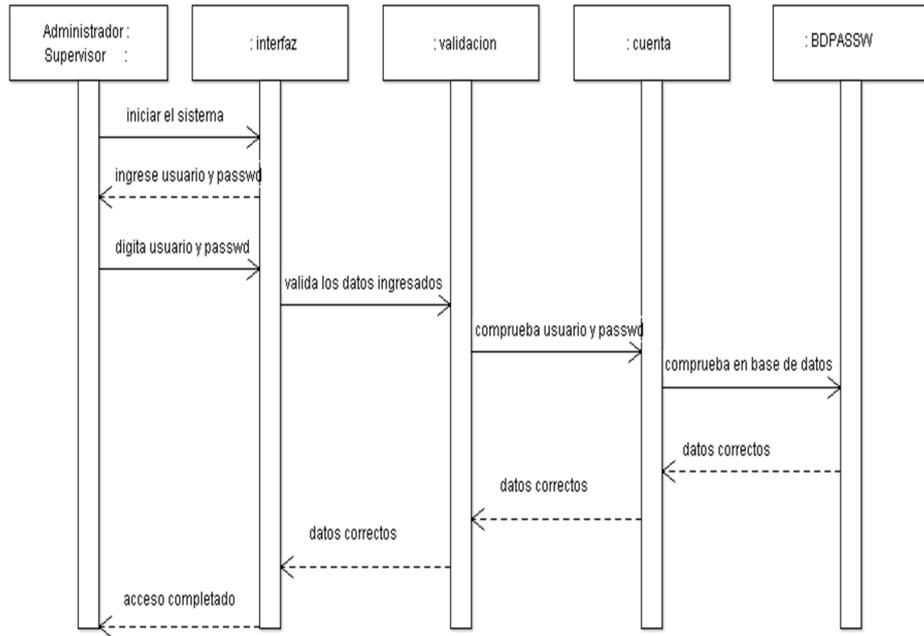
Gráfico Nro. 32: CU09 Generar Backup del sistema



Fuente: Elaboración propia

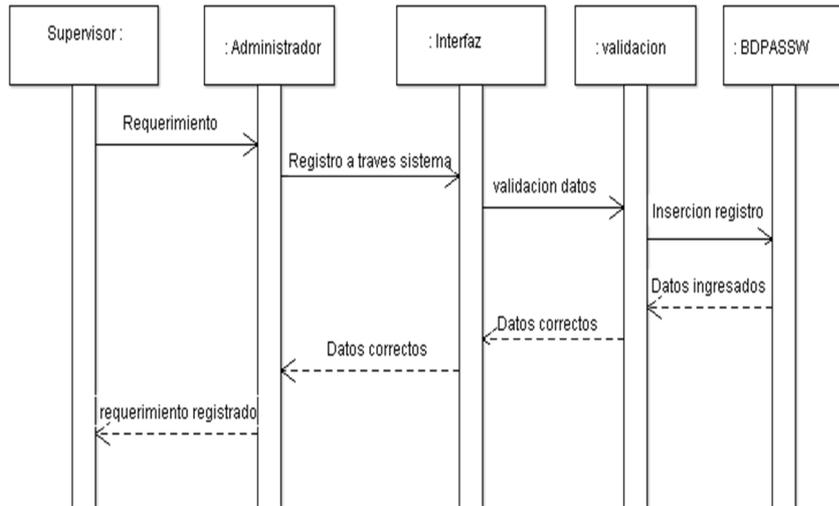
Actividades.-

Gráfico Nro. 33: Diagrama de Secuencia - Ingresar al sistema



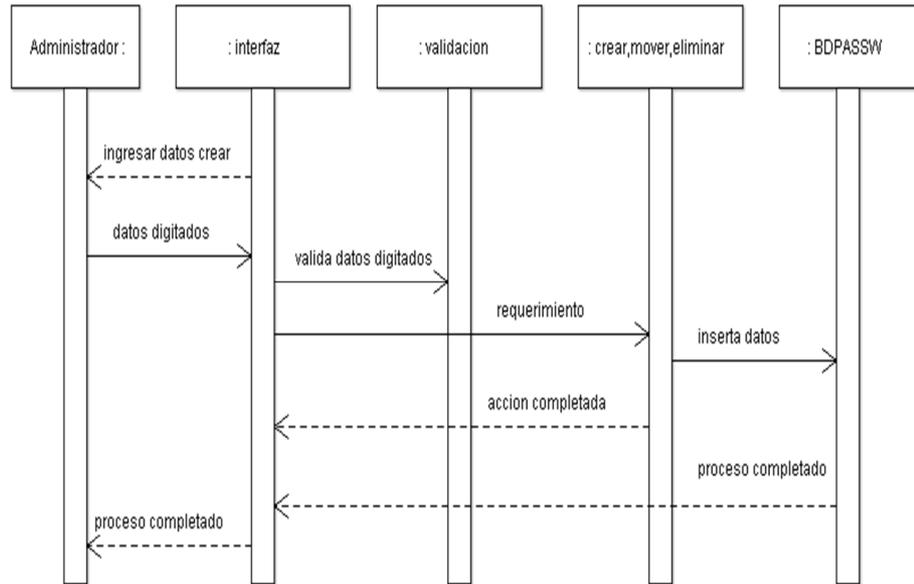
Fuente: elaboración propia.

Gráfico Nro. 34: Diagrama de Secuencia – Requerimiento crear usuario.



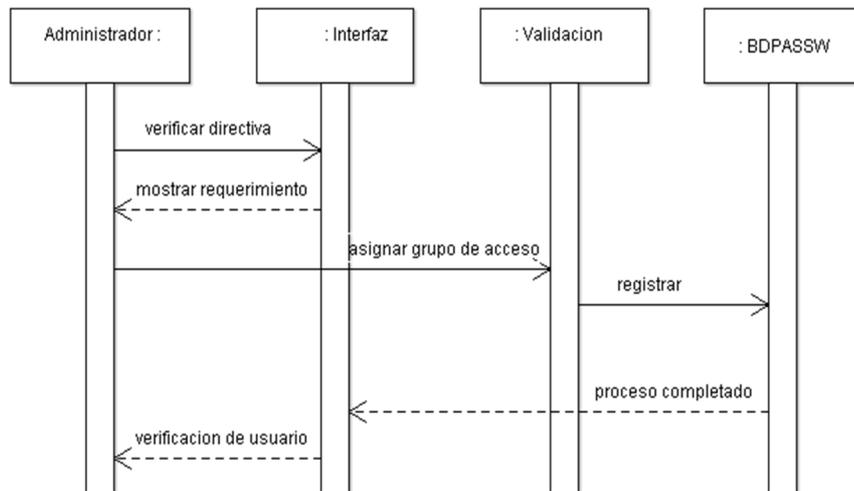
Fuente: Elaboración propia.

Gráfico Nro. 35: Diagrama de Secuencia - Crear usuario



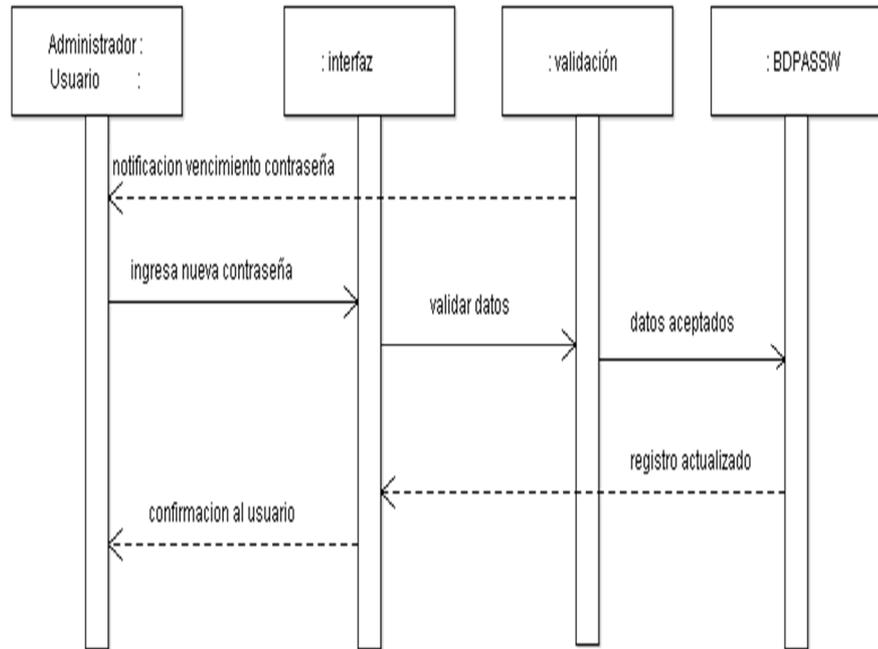
Fuente: Elaboración propia.

Gráfico Nro. 36: Diagrama de Secuencia - Asignar nivel de usuario.



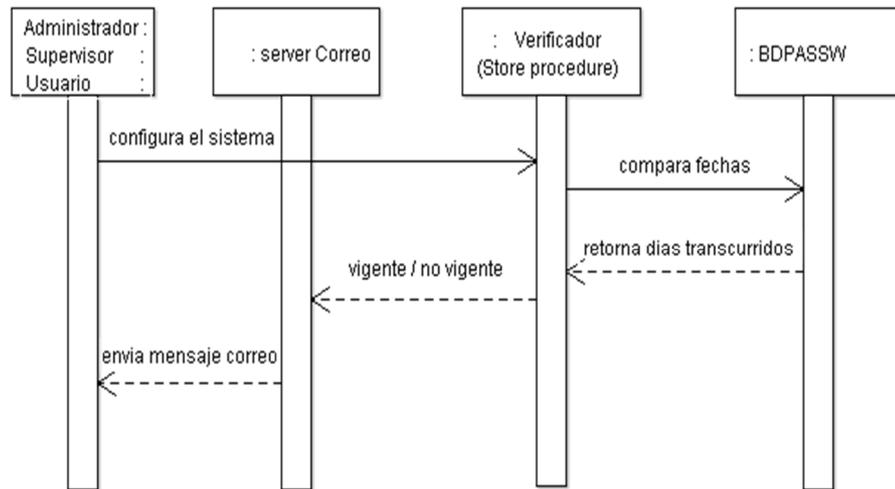
Fuente: Elaboración propia.

Gráfico Nro. 37: Diagrama de Secuencia - Cambiar contraseña



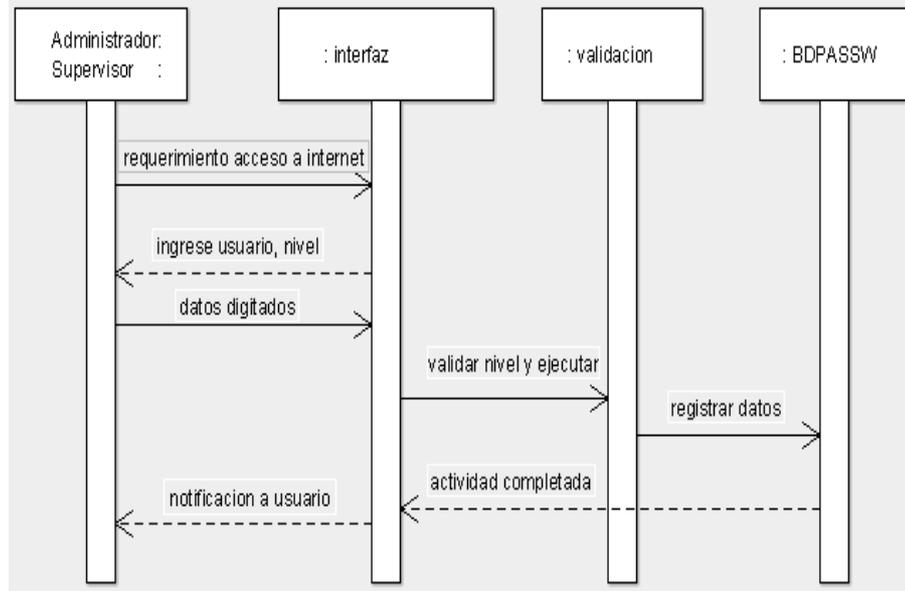
Fuente: Elaboración propia.

Gráfico Nro. 38: Diagrama de Secuencia - Verificar vigencia de contraseña



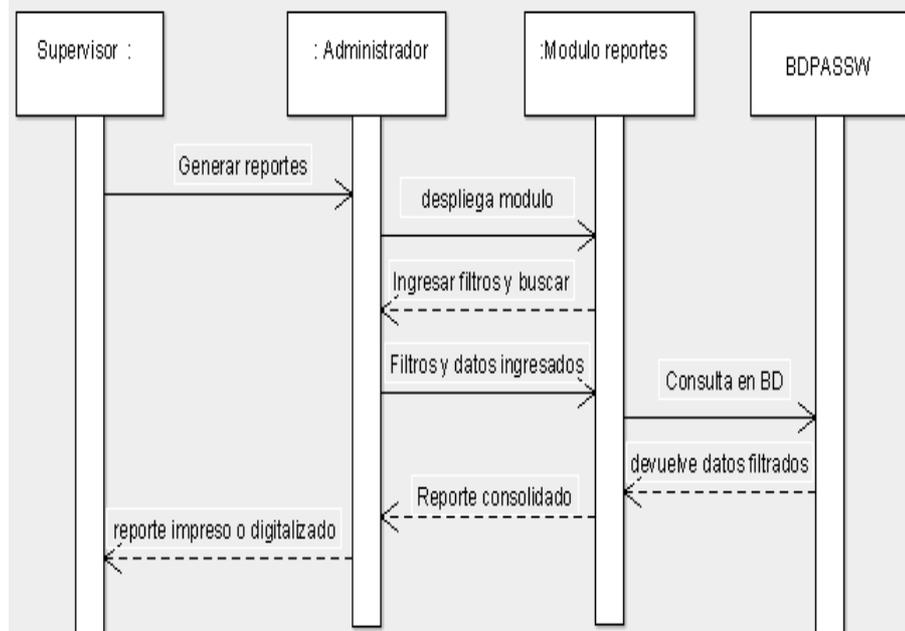
Fuente: Elaboración propia.

Gráfico Nro. 39: Diagrama de Secuencia - Controlar acceso a internet.



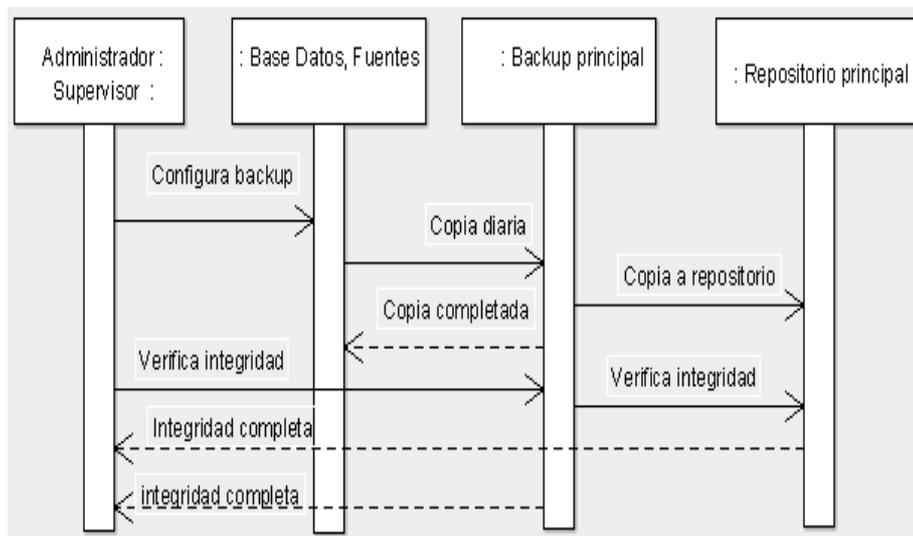
Fuente: Elaboración propia

Gráfico Nro. 40: Diagrama Secuencia – Generar reportes.



Fuente: Elaboración propia

Gráfico Nro. 41: Diagrama de Secuencia – Generar backup del sistema.



Fuente: elaboración propia

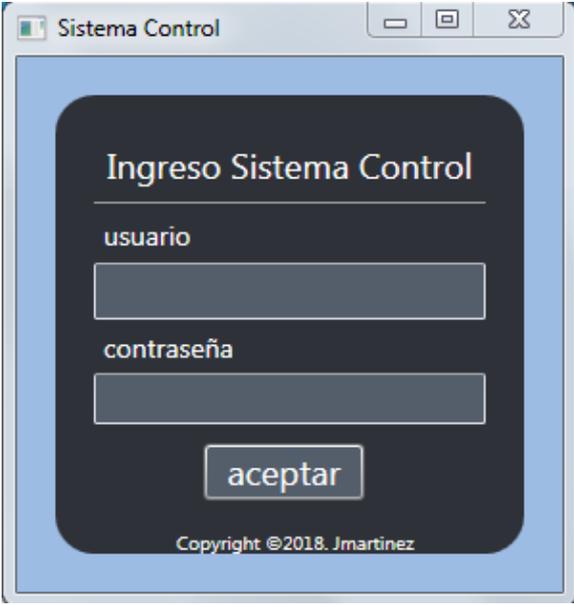
5.3.5. Interfaces

Ingresar al sistema.-

Presenta controles que deben ser digitados por el usuario administrador previamente designado por la Jefatura DTIC, ver Gráfico Nro. 42.

- Cuadro de texto “usuario”, aquí se digita la cuenta de usuario administrador.
- Cuadro de texto “contraseña”, aquí digita contraseña asignada.
- Botón “aceptar”, sirve para enviar los datos digitados, que luego serán comparados con los almacenados en la base de datos, si hay coincidencia el sistema muestra el menú mostrado en el gráfico 27.

Gráfico Nro. 42: Ingresar al sistema

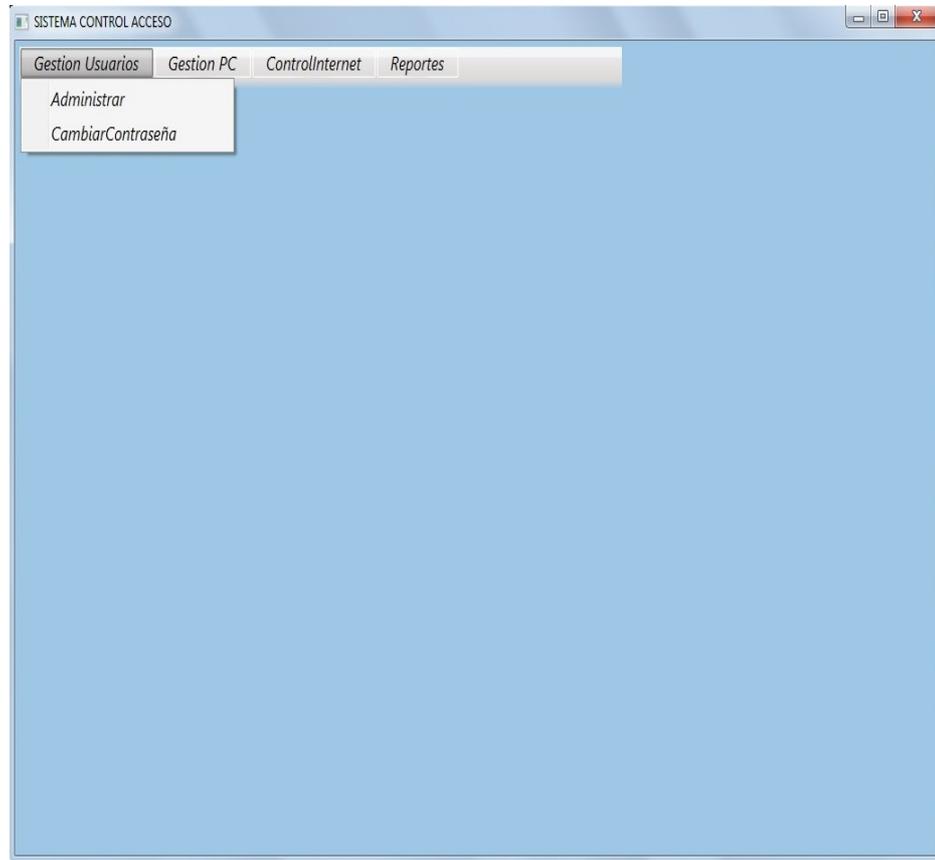


The image shows a screenshot of a web application window titled "Sistema Control". The main content area has a dark blue background with a light blue border. At the top, it says "Ingreso Sistema Control". Below this, there are two input fields: one labeled "usuario" and another labeled "contraseña". Below the input fields is a button labeled "aceptar". At the bottom of the dark blue area, there is a small text that reads "Copyright ©2018. Jmartinez". The window also shows standard OS window controls (minimize, maximize, close) in the top right corner.

Fuente: Elaboración propia

Menú del sistema.-

Gráfico Nro. 43: Menú de sistema



Fuente: Elaboración propia

Consta de opciones para desplegar tales como:

- “Gestión usuarios”, que presenta un submenú "administrar" con lo cual se despliega el formulario Gestión Usuarios.

Gráfico Nro. 44: Formulario gestión de usuarios

The screenshot shows a web application window titled "SISTEMA CONTROL ACCESO: Gestion Usuarios". The window contains the SIMA logo in the top left corner. The form includes the following fields and controls:

- Seleccionar Area:** A dropdown menu.
- CuentaUsuario:** A text input field.
- ConfirmarCuentaUsuario:** A text input field.
- Contraseña:** A text input field.
- PrimerNombre:** A text input field.
- Apellidos:** A text input field.
- Cargo:** A text input field.
- HabilitarUsuario:** A radio button.
- CrearUsuario:** A button.
- EliminarUsuario:** A button.
- LimpiarForm:** A button.
- Cerrar:** A button.

Copyright ©2018. Jmartinez

Fuente: Elaboración propia

- “Cambiar contraseña”, despliega el formulario cambiar contraseña usuario, permitiendo cambiar contraseña de los usuarios según requerimiento, así mismo el usuario puede cambiar su contraseña de acceso a red a través del aplicativo enviado por el sistema a su correo.

Gráfico Nro. 45: Formulario cambiar contraseña.

The image shows a web application window titled "SISTEMA CONTROL ACCESO: Cambiar Contraseña Usuario". The interface is light blue and contains the following elements:

- Logo:** The SIMA logo, consisting of a blue diamond shape with a white arrow pointing right, followed by the text "SIMA" in a bold, blue, sans-serif font.
- User Icon:** An illustration of a man in a suit holding a large golden key.
- Form Fields:** Four white input fields with labels to their left:
 - "Cuenta de Usuario:"
 - "Contraseña Anterior:"
 - "Nueva Contraseña:"
 - "Confirmar Contraseña:"
- Buttons:** Two buttons at the bottom: "Guardar" (left) and "Cerrar" (right).
- Copyright:** "Copyright ©2018. Jmartinez" located at the bottom right of the window.

Fuente: Elaboración propia.

Gestión PC.-

- Despliega el formulario "Gestión PC" que permite realizar reubicaciones entre áreas, dar de baja en la red.

Gráfico Nro. 46: Formulario Gestión Pc



The image shows a screenshot of a web application window titled "SISTEMA CONTROL ACCESO: Gestion PC". The window has a blue background and a logo for "SIMA" in the top left corner. The form contains several input fields and buttons:

- Directorio inicio:** A text input field.
- Directorio Destino:** A text input field.
- CuentaUsuario:** A text input field.
- ConfirmaCuentaUsuario:** A text input field.
- Nombre de PC:** A text input field.
- HabilitarPC:** A radio button.
- Mover PC:** A button.
- Limpiar Form:** A button.
- Cerrar:** A button.

On the right side of the form, there is a circular icon of a laptop. At the bottom right, there is a copyright notice: "Copyright ©2018. Jmartinez".

Fuente: Elaboración propia

Control Internet.-

- Despliega el formulario Control internet que permite gestionar el acceso a internet según niveles requeridos.

Gráfico Nro. 47: Formulario Control Internet

SISTEMA CONTROL ACCESO: Control Internet

SIMA

Grupo Internet inicial:

Grupo Internet Final:

CuentaUsuario:

ConfirmaCuentaUsuario:

Asignar Internet

Limpiar Form Cerrar

Copyright ©2018. Jmartinez

Fuente: Elaboración propia

Reportes.-

- Despliega el formulario reportes que permite realizar búsquedas por área, por usuario, para luego generar.

Gráfico Nro. 48: Formulario reportes

SISTEMA CONTROL ACCESO: Reportes

SIMA

Reportes por

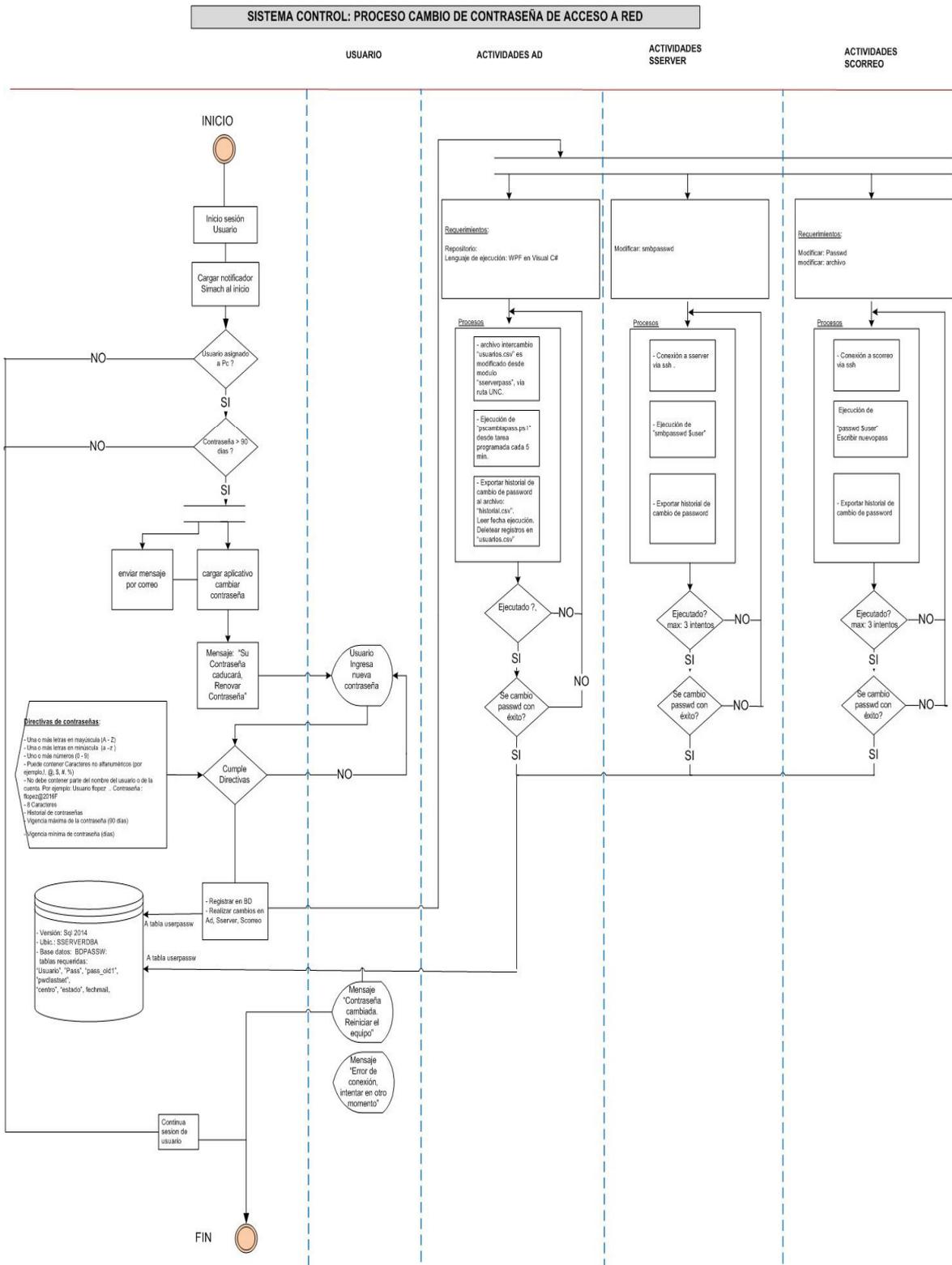
Area

Usuario

Copyright ©2018. Jmartinez

Fuente: Elaboración propia

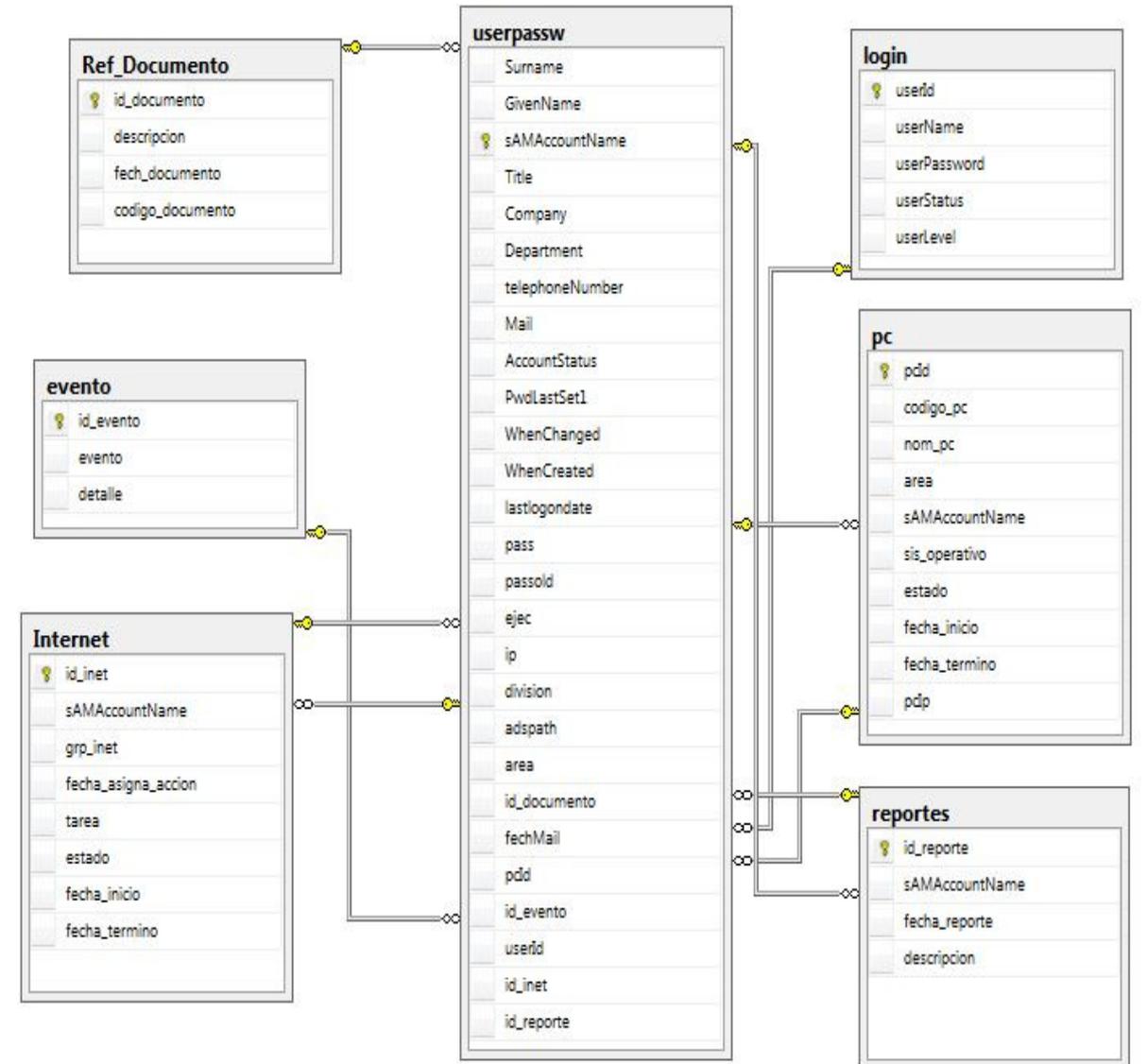
Gráfico Nro. 49: Diagrama de Flujo de proceso



Fuente: Elaboración propia

Diagrama de la base de datos.-

Gráfico Nro. 50: Diagrama de Base de Datos



Fuente: Elaboración propia.

Programación del sistema de control de acceso a red.-

Módulo de autenticación inicial

```
////////////////////////////////////  
LoginScreen.xalm
```

```
<Window x:Class="wpfloginscreen.LoginScreen"  
  xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"  
    xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"  
      Title="SISTEMA CONTROL ACCESO: Ingreso"  
  Height="319" Width="300" FontSize="14"  
  Background="#FF9DBCE4"  
  WindowStartupLocation="CenterScreen">  
    <Border Background="#2e3137" CornerRadius="20"  
  Margin="20">  
      <StackPanel Margin="20,20,20,0">  
        <Label Content="Ingreso Sistema Control"  
  Foreground="White" FontSize="18"  
  HorizontalAlignment="Center"/>  
        <Separator/>  
        <Label Content="usuario" Foreground="White"/>  
        <TextBox Name="txtUsername"  
  Background="#545d6a" Foreground="White" FontSize="18"  
  TextChanged="txtUsername_TextChanged"/>  
        <Label Content="contraseña" Foreground="White"/>  
        <PasswordBox Name="txtPassword"  
  Background="#545d6a" Foreground="White" FontSize="18"/>  
        <Button x:Name="btnSubmit"  
  Click="btnSubmit_Click" Content="aceptar" Margin="57,10,63,10"  
  Background="#545d6a" Foreground="White" FontSize="14"/>  
        <Label Content="Copyright ©2018. Jmartinez"  
  HorizontalAlignment="Left" Height="24" Width="142"  
  Foreground="#FFF9F9F9" FontSize="10" Margin="38,0,0,0"/>
```

```

        </StackPanel>
    </Border>
</Window>
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
LoginScreen.xalm.cs

using System;
using System.Collections.Generic;
using System.Data;
using System.Data.SqlClient;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows;
using System.Windows.Controls;
using System.Windows.Data;
using System.Windows.Documents;
using System.Windows.Input;
using System.Windows.Media;
using System.Windows.Media.Imaging;
using System.Windows.Shapes;

namespace wpfloginscreen
{
    /// <summary>
    /// Interaction logic for LoginScreen.xaml
    /// </summary>
    public partial class LoginScreen : Window
    {
        public LoginScreen()
        {
            InitializeComponent();

            // this.Logger =
            LogManager.GetLogger(Assembly.GetExecutingAssembly().GetTypes()
            s().First());
            log4net.Config.XmlConfigurator.Configure();
            // this.Logger.Info("Inicio de la app");
        }
        private void btnSubmit_Click(object sender, RoutedEventArgs e)
        {
            SqlConnection sqlCon = new SqlConnection(@"Data
            Source=pc10003\sqlserver; Initial Catalog=BDPASSW; Integrated
            Security=True;");
            try
            {

```

```

        if (sqlCon.State == ConnectionState.Closed)
            sqlCon.Open();
        String query = "SELECT COUNT(1) FROM login WHERE
userName=@Username AND userPassword=@Password";
        SqlCommand sqlCmd = new SqlCommand(query, sqlCon);
        sqlCmd.CommandType = CommandType.Text;
sqlCmd.Parameters.AddWithValue("@Username",txtUsername.Text);
        sqlCmd.Parameters.AddWithValue("@Password",
txtPassword.Password);
        int count = Convert.ToInt32(sqlCmd.ExecuteScalar());
        if (count == 1)
        {
            MainWindow dashboard = new MainWindow();
            dashboard.Show();
            this.Close();
        }
        else
        {
            MessageBox.Show("Username or password is
incorrect.");
            txtUsername.Clear(); //limpiar caja
            txtPassword.Clear();
        }
    }
    catch (Exception ex)
    {
        MessageBox.Show(ex.Message);
    }
    finally
    {
        sqlCon.Close();
    }
}
private void txtUsername_TextChanged(object sender,
TextChangedEventArgs e)
{
}
}
}
////////////////////////////////////

```

MainWindow.xaml

```

<Window x:Class="wpfloginscreen.MainWindow"
xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"

xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"

```

```

Title="SISTEMA CONTROL ACCESO" Height="627"
Width="1036.701" Background="#FF9DC7E4" FontSize="14"
WindowStartupLocation="CenterScreen">
  <Grid>
    <Grid.ColumnDefinitions>
      <ColumnDefinition Width="7*"/>
      <ColumnDefinition Width="254*"/>
      <ColumnDefinition Width="82*"/>
    </Grid.ColumnDefinitions>
    <Label Grid.ColumnSpan="3">
      <Label.BorderBrush>
        <LinearGradientBrush EndPoint="0.5,1"
StartPoint="0.5,0">
          <GradientStop Color="Black" Offset="0"/>
          <GradientStop Color="White" Offset="1"/>
        </LinearGradientBrush>
      </Label.BorderBrush>
      <Menu Height="34" Width="667">
        <Menu.Background>
          <LinearGradientBrush EndPoint="0,1"
StartPoint="0,0">
            <GradientStop Color="#FFF6F6F6"
Offset="0.25"/>
            <GradientStop Color="#FFEAE8E8"
Offset="0.25"/>
            <GradientStop Color="#FFDCD9D9"
Offset="0.8"/>
            <GradientStop Color="#FF9DC7E4"
Offset="1"/>
          </LinearGradientBrush>
        </Menu.Background>
        <MenuItem Header=" Gestion Usuarios "
FontSize="16" FontStyle="Italic">
          <MenuItem.BorderBrush>
            <RadialGradientBrush>
              <GradientStop Color="Black" Offset="0"/>
              <GradientStop Color="White" Offset="1"/>
            </RadialGradientBrush>
          </MenuItem.BorderBrush>
          <MenuItem Header="Administrar"
Click="MenuItem_Click_1"/>
          <MenuItem Header="CambiarContraseña"
Click="MenuItem_Click_2"/>
          <MenuItem Header="Documentos Ref."
Click="MenuItem_Click_6"/>
        </MenuItem>
        <MenuItem Header=" Gestion PC " FontSize="16"
FontStyle="Italic">

```

```

        <MenuItem.BorderBrush>
            <RadialGradientBrush>
                <GradientStop Color="Black" Offset="0"/>
                <GradientStop Color="White" Offset="1"/>
            </RadialGradientBrush>
        </MenuItem.BorderBrush>
        <MenuItem Header="Administrar"
Click="MenuItem_Click_3"/>
    </MenuItem>
    <MenuItem Header=" ControlInternet "
FontSize="16" FontStyle="Italic">
        <MenuItem.BorderBrush>
            <RadialGradientBrush>
                <GradientStop Color="Black" Offset="0"/>
                <GradientStop Color="White" Offset="1"/>
            </RadialGradientBrush>
        </MenuItem.BorderBrush>
        <MenuItem Header="Administrar"
Click="MenuItem_Click_4"/>
    </MenuItem>
    <MenuItem Header=" Reportes " FontSize="16"
FontStyle="Italic">
        <MenuItem.BorderBrush>
            <RadialGradientBrush>
                <GradientStop Color="Black" Offset="0"/>
                <GradientStop Color="White" Offset="1"/>
            </RadialGradientBrush>
        </MenuItem.BorderBrush>
        <MenuItem Header="Generar"
Click="MenuItem_Click_5"/>
    </MenuItem>
</Menu>
</Label>
</Grid>
</Window>
////////////////////////////////////////////////////////////////

```

MainWindow.xalm.cs

```

using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows;
using System.Windows.Controls;
using System.Windows.Data;
using System.Windows.Documents;

```

```

using System.Windows.Input;
using System.Windows.Media;
using System.Windows.Media.Imaging;
using System.Windows.Navigation;
using System.Windows.Shapes;

namespace wpfloginscreen
{
    /// <summary>
    /// Interaction logic for MainWindow.xaml
    /// </summary>
    public partial class MainWindow : Window
    {
        public MainWindow()
        {
            InitializeComponent();
        }
        private void MenuItem_Click(object sender, RoutedEventArgs e)
        {

        }

        private void MenuItem_Click_1(object sender,
RoutedEventArgs e)
        {
            ActiveDirectoryTest.MainWindow p = new
ActiveDirectoryTest.MainWindow();
            p.Show();

        }
        private void MenuItem_Click_2(object sender,
RoutedEventArgs e)
        {

            adcambiapass.MainWindow modalc = new
adcambiapass.MainWindow();
            modalc.Owner = this;
            modalc.ShowDialog();

        }

        private void MenuItem_Click_3(object sender,
RoutedEventArgs e)
        {
            adpc.MainWindow modalp = new
adpc.MainWindow();

            modalp.Owner = this;
            modalp.ShowDialog();
        }
    }
}

```

```

    }
    private void MenuItem_Click_4(object sender,
RoutedEventArgs e)
    {

    }

    private void MenuItem_Click_5(object sender,
RoutedEventArgs e)
    {
        // private void LlamarModalClick(object sender,
RoutedEventArgs e)
        // {
            AdReportes.MainWindow modal = new
AdReportes.MainWindow();
            modal.Owner = this;
            modal.ShowDialog();

        // }
    }

    private void MenuItem_Click_6(object sender, RoutedEventArgs
e)
    {

    }
}

```

//

Modulo Gestión de usuarios

MainWindow.xaml

<Window x:Class="ActiveDirectoryTest.MainWindow"

xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
SizeToContent="WidthAndHeight"
Title="SISTEMA CONTROL ACCESO: Gestion Usuarios"
Height="627.462" Width="753.462" Loaded="Window_Loaded_1"
Icon="System.ico" ShowInTaskbar="False" FontSize="14"
Background="#FF9DC7E4" WindowStartupLocation="CenterScreen"
Focusable="False">

<Grid>
<Button x:Name="button1" Content="AgregarUsuario"
HorizontalAlignment="Left" Margin="20,541,0,0"

```

VerticalAlignment="Top" Width="107" Click="button1_Click"
Visibility="Hidden"/>
    <TextBox x:Name="textboxSamAccountName"
HorizontalAlignment="Left" Height="27" Margin="321,164,0,0"
TextWrapping="Wrap" VerticalAlignment="Top" Width="219"
TabIndex="5" MaxLength="30"/>
    <TextBox x:Name="textboxLonOnName"
HorizontalAlignment="Left" Height="27" Margin="320,120,0,0"
TextWrapping="Wrap" VerticalAlignment="Top" Width="219"
TabIndex="4" MaxLength="30" MinLines="2"/>
    <TextBox x:Name="textboxAdminUsername"
HorizontalAlignment="Left" Height="22" Margin="124,12,0,0"
TextWrapping="Wrap" VerticalAlignment="Top" Width="153"
TabIndex="1" Text="empresa\user" Visibility="Hidden"/>
    <PasswordBox x:Name="passwordboxAdminPassword"
HorizontalAlignment="Left" Height="22" Margin="124,45,0,0"
VerticalAlignment="Top" Width="153" TabIndex="2"
Password="xxxxxxx" Visibility="Hidden"/>
    <Label Content="Admin User:" HorizontalAlignment="Left"
Margin="52,51,0,0" VerticalAlignment="Top" Width="98"
Visibility="Hidden"/>
    <Label Content="Admin Pass:" HorizontalAlignment="Left"
Margin="53,84,0,0" VerticalAlignment="Top" Width="98"
Visibility="Hidden"/>
    <Label Content="Apellidos, Nombre: "
HorizontalAlignment="Left" Margin="44,294,0,0"
VerticalAlignment="Top" Width="137" Visibility="Hidden"/>
    <Label Content="Contraseña:" HorizontalAlignment="Left"
Margin="89,220,0,0" VerticalAlignment="Top" Width="92"/>
    <TextBox x:Name="textboxOu" HorizontalAlignment="Left"
Height="50" Margin="174,77,0,0" TextWrapping="Wrap"
VerticalAlignment="Top" Width="295" FontSize="12" TabIndex="3"
MaxLength="200" Visibility="Hidden"/>
    <Label Content="Directorio: " HorizontalAlignment="Left"
Margin="94,77,0,0" VerticalAlignment="Top" Visibility="Hidden"/>
    <Label Content="ConfirmarCuentaUsuario:"
HorizontalAlignment="Left" Margin="149,162,0,0"
VerticalAlignment="Top" Width="170"/>
    <TextBox x:Name="textboxName" HorizontalAlignment="Left"
Height="27" Margin="175,296,0,0" TextWrapping="Wrap"
VerticalAlignment="Top" Width="219" TabIndex="7"
Visibility="Hidden"/>
    <TextBox x:Name="textboxGivenName"
HorizontalAlignment="Left" Height="27" Margin="175,265,0,0"
TextWrapping="Wrap" VerticalAlignment="Top" Width="219"
TabIndex="8" MaxLength="30"/>
    <TextBox x:Name="textboxSurname"
HorizontalAlignment="Left" Height="27" Margin="176,309,0,0"

```

```

TextWrapping="Wrap" VerticalAlignment="Top" Width="219"
TabIndex="9" MaxLength="30"/>
    <Label Content="PrimerNombre: " HorizontalAlignment="Left"
Margin="66,263,0,0" VerticalAlignment="Top" Width="108"/>
    <Label Content="Apellidos: " HorizontalAlignment="Left"
Margin="100,307,0,0" VerticalAlignment="Top" Width="74"/>
    <TextBox x:Name="textboxDescription"
HorizontalAlignment="Left" Height="27" Margin="177,353,0,0"
TextWrapping="Wrap" VerticalAlignment="Top" Width="219"
TabIndex="11" MaxLength="100"/>
    <Label Content="Cargo: " HorizontalAlignment="Left"
Margin="119,351,0,0" VerticalAlignment="Top" Width="54"/>
    <RadioButton x:Name="radiobuttonEnable"
Content="HabilitarUsuario" HorizontalAlignment="Left"
Margin="242,430,0,0" VerticalAlignment="Top"
IsChecked="True"/>
    <PasswordBox x:Name="passwordboxUserPass"
HorizontalAlignment="Left" Height="27" Margin="175,222,0,0"
VerticalAlignment="Top" Width="219" TabIndex="6"
MaxLength="8"/>
    <Label Content="Documento Ref:" HorizontalAlignment="Left"
Margin="59,395,0,0" VerticalAlignment="Top" Width="110"/>
    <TextBox x:Name="txtRefdocumento"
HorizontalAlignment="Left" Height="27" Margin="177,395,0,0"
TextWrapping="Wrap" VerticalAlignment="Top" Width="219"
TabIndex="4" MaxLength="30" MinLines="2"/>
    <Label Content="CuentaUsuario:" HorizontalAlignment="Left"
Margin="211,120,0,0" VerticalAlignment="Top" Width="104"/>
    <TextBox x:Name="textboxDisplayName"
HorizontalAlignment="Left" Height="27" Margin="177,410,0,0"
TextWrapping="Wrap" VerticalAlignment="Top" Width="219"
TabIndex="10" MaxLength="50" Visibility="Hidden"/>
    <Label Content="Nombre para mostrar:"
HorizontalAlignment="Left" Margin="20,409,0,0"
VerticalAlignment="Top" Width="155" Visibility="Hidden"/>
    <Image HorizontalAlignment="Left" Height="56"
Margin="0,2,0,0" VerticalAlignment="Top" Width="150"
Source="d:\LogoSima.jpg"/>
    <Button x:Name="btnCerrar" Content="Cerrar"
HorizontalAlignment="Left" Margin="431,525,0,0"
VerticalAlignment="Top" Width="75" Click="btnCerrar_Click"/>
    <Button x:Name="btnCrear" Content="CrearUsuario"
HorizontalAlignment="Left" Margin="242,458,0,0"
VerticalAlignment="Top" Width="101" Click="btnCrear_Click"
Height="40"/>
    <Button x:Name="btnCleanad" Content="LimpiarForm"
HorizontalAlignment="Left" Margin="295,525,0,0"
VerticalAlignment="Top" Width="101"/>

```

```

        <Label Content="Copyright ©2018. Jmartinez"
HorizontalAlignment="Left" Height="35" Margin="561,569,0,0"
VerticalAlignment="Top" Width="181" FontSize="12"/>
        <Button x:Name="btnEliminar" Content="EliminarUsuario"
HorizontalAlignment="Left" Margin="529,458,0,0"
VerticalAlignment="Top" Width="104" Click="btnEliminar_Click"
Height="40"/>
        <Label Content="Seleccionar Area:"
HorizontalAlignment="Left" Margin="197,64,0,0"
VerticalAlignment="Top" Width="118"/>
        <ComboBox x:Name="cmbArea" HorizontalAlignment="Left"
Margin="322,68,0,0" VerticalAlignment="Top" Width="120" >
        <ComboBoxItem
Content="...seleccionar"></ComboBoxItem>
        <ComboBoxItem Content="dtic"></ComboBoxItem>
        <ComboBoxItem Content="joesch"></ComboBoxItem>
        </ComboBox>
        <Rectangle HorizontalAlignment="Left" Height="279"
Margin="418,211,0,0" Stroke="#FFFBFBFB"
VerticalAlignment="Top" Width="4">
        <Rectangle.Fill>
        <RadialGradientBrush>
        <GradientStop Color="#FF007AFF" Offset="0"/>
        <GradientStop Color="#FF00B4FF" Offset="1"/>
        <GradientStop Color="#FF00E2FF" Offset="1"/>
        </RadialGradientBrush>
        </Rectangle.Fill>
        </Rectangle>

</Grid>
</Window>

```

```

////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

```

```

MainWindow.xalm.cs

```

```

using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows;
using System.Windows.Controls;
using System.Windows.Data;
using System.Windows.Documents;
using System.Windows.Input;
using System.Windows.Media;
using System.Windows.Media.Imaging;

```

```

using System.Windows.Navigation;
using System.Windows.Shapes;

using System.DirectoryServices.AccountManagement;
using Tamir.SharpSsh;
using System.Text.RegularExpressions;
using System.Data.SqlClient;

namespace ActiveDirectoryTest
{
    /// <summary>
    /// Interaction logic for MainWindow.xaml
    /// </summary>
    public partial class MainWindow : Window
    {
        public MainWindow()
        {
            InitializeComponent();
        }
        private void button1_Click(object sender, RoutedEventArgs e)
        {
            try
            {
                string stringDomainName =
System.Net.NetworkInformation.IPGlobalProperties.GetIPGlobalProp
erties().DomainName;
                PrincipalContext PrincipalContext4 = new
PrincipalContext(ContextType.Domain, stringDomainName,
textboxOu.Text, ContextOptions.SimpleBind,
textboxAdminUsername.Text,
passwordboxAdminPassword.Password);
                UserPrincipal UserPrincipal1 = new
UserPrincipal(PrincipalContext4, textboxLonOnName.Text,
passwordboxUserPass.Password, true);
                UserPrincipal1.UserPrincipalName =
textboxSamAccountName.Text;
                // UserPrincipal1.Name = textboxName.Text;
                // UserPrincipal1.Name = textboxSurname.Text+" "+
textboxGivenName.Text;
                UserPrincipal1.GivenName = textboxGivenName.Text;
                UserPrincipal1.Surname = textboxSurname.Text;
                UserPrincipal1.Name = textboxSurname.Text+" "+
textboxGivenName.Text;
                UserPrincipal1.DisplayName = textboxSurname.Text+" "+
textboxGivenName.Text;
                UserPrincipal1.Description = textboxDescription.Text;
                if (radiobuttonEnable.IsChecked == true)
                {

```

```

        UserPrincipal1.Enabled = true;
    }
    else
    {
        UserPrincipal1.Enabled = false;
    }
    UserPrincipal1.Save();
    MessageBox.Show("Proceso Guardado");
}
catch (Exception ex)
{
    MessageBox.Show(ex.ToString());
}
}
private void Window_Loaded_1(object sender, RoutedEventArgs
e)
{
    //textboxOu.Text = ",OU=Basic,OU=Chimbote,OU=Users
empresa,DC=empresa,DC=com,DC=pe";
    textboxOu.Text =
"OU="+Convert.ToString(cmbArea.SelectedItem)+"",OU=Basic,OU=
Chimbote,OU=Users empresa,DC=empresa,DC=com,DC=pe";
}
private void btnCrear_Click(object sender, RoutedEventArgs e)
{
    ///////////validar campos vacios
    if (string.IsNullOrEmpty(textboxLonOnName.Text) ||
string.IsNullOrEmpty(textboxSamAccountName.Text) ||
string.IsNullOrEmpty(txtRefdocumento.Text) ||
string.IsNullOrEmpty(textboxGivenName.Text) ||
string.IsNullOrEmpty(textboxSurname.Text) ||
string.IsNullOrEmpty(textboxDescription.Text))
    {
        MessageBox.Show("Debe completar la informacion");
        return;
    }
    //////////////////////////////////////CONEXION SQL
    try
    {
        //SqlConnection conexion = new
SqlConnection("server=sserverdba\\sserverdba; database=simachdb;
integrated security = true");
        SqlConnection conexion = new SqlConnection("data source
= pc10003\\sqlserver; initial catalog = BDPASSW; user id = usersql;
password = xxxxxx");
    }
}

```

```

        conexion.Open();
        //MessageBox.Show("conexión SQL + BD SisControl");
        string sql = @"INSERT INTO userpassw (Surname,
GivenName, sAMAccountName, Title, Company, Department,
telephoneNumber, Mail, AccountStatus, PwdLastSet1,
WhenChanged, WhenCreated, lastlogondate, pass, passold, ejec, ip,
division, adspath, area, id_documento, fechMail, pcId, id_evento,
userId, id_inet, id_reporte)
            VALUES ('" + textboxSurname.Text + "','" +
textboxGivenName.Text + "','" + textboxSamAccountName.Text +
"',"' + textboxDescription.Text + "','Sima Chimbote',NULL,'350721','"
+ textboxSamAccountName.Text +
"@sima.com.pe','Enabled',getdate(),'19-03-2018',getdate(),getdate(),'"
+ passwordboxUserPass.Password + "','" +
passwordboxUserPass.Password + "','NULL,NULL','A','" +
textboxOu.Text + "','" + Convert.ToString(cmbArea.SelectedItem) +
"',NULL,NULL,NULL,NULL,NULL,NULL,NULL)";
        SqlCommand command = new SqlCommand(sql,
conexion);
        command.Parameters.AddWithValue("USUARIO",
textboxSamAccountName.Text);
        command.Parameters.AddWithValue("CLAVE",
passwordboxUserPass.Password);
        command.ExecuteNonQuery();
        MessageBox.Show("Usuario '" +
textboxSamAccountName.Text + "' creado en BD");
        conexion.Close();
        MessageBox.Show("Se cerró la conexión.");

        //////////CREAR EN AD
        try
        {
            string stringDomainName =
System.Net.NetworkInformation.IPGlobalProperties.GetIPGlobalProp
erties().DomainName;
            PrincipalContext PrincipalContext4 = new
PrincipalContext(ContextType.Domain, stringDomainName,
textboxOu.Text, ContextOptions.SimpleBind,
textboxAdminUsername.Text,
passwordboxAdminPassword.Password);
            UserPrincipal UserPrincipal1 = new
UserPrincipal(PrincipalContext4, textboxLonOnName.Text,
passwordboxUserPass.Password, true);

            UserPrincipal1.UserPrincipalName =
textboxSamAccountName.Text;
            //UserPrincipal1.Name = textboxName.Text;
            UserPrincipal1.GivenName = textboxGivenName.Text;

```

```

        UserPrincipal1.Surname = textboxSurname.Text;
        UserPrincipal1.Name = textboxSurname.Text + "," +
textboxGivenName.Text;
        UserPrincipal1.DisplayName = textboxSurname.Text +
"," + textboxGivenName.Text;
        //UserPrincipal1.DisplayName =
textboxDisplayName.Text;
        UserPrincipal1.Description = textboxDescription.Text;
        if (radiobuttonEnable.IsChecked == true)
        {
            UserPrincipal1.Enabled = true;
            MessageBox.Show(textboxOu.Text);
        }
        else
        {
            UserPrincipal1.Enabled = false;
        }
        UserPrincipal1.Save();
        MessageBox.Show("1. Paso: usuario " +
textboxSamAccountName.Text + " creado en AD");

/////////CREAR EN SSERVER
const string host = "10.30.0.254";
const string passSamba = "passw";
const string admin = "user";
Console.WriteLine("OK");
try
{
    SshExec sshExec = new SshExec(host, admin,
passSamba); //
    sshExec.Connect();
    sshExec.Close();
    Console.WriteLine(".....");
    SshExec exec = new SshExec(host, admin);
    exec.Password = passSamba;
    exec.Connect();
    Console.Write("Connecting...");
    string comando1 = "/usr/sbin/useradd " +
textboxSamAccountName.Text;
    exec.RunCommand(comando1);
    string comando2 = "(echo " +
passwordboxUserPass.Password + "; echo " +
passwordboxUserPass.Password + ") | smbpasswd -as " +
textboxSamAccountName.Text;
    exec.RunCommand(comando2);

    Console.Write(comando1);
    MessageBox.Show(comando1);

```

```

        Console.WriteLine(commando2);
        MessageBox.Show(commando2);

        exec.Close();
        Console.WriteLine("Disconnecting...");
        MessageBox.Show("2. Paso: Crear Usuario en
SSERVER");

```

```

////////////////////////////////////

```

Modulo Cambiar Contraseñas

MainWindow.xaml

```

<Window x:Class="adcambiapass.MainWindow"

xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
    xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
    Title="SISTEMA CONTROL ACCESO: Cambiar Contraseña
Usuario" Height="591" Width="604" FontSize="14"
WindowStartupLocation="CenterScreen">
    <Grid Background="#FF9DC7E4" Margin="0,0,0,1">

        <Button x:Name="button1" Content="Conectar AD"
HorizontalAlignment="Left" Margin="40,569,0,0"
VerticalAlignment="Top" Width="115" Click="button1_Click"
FontSize="14" Height="36" Visibility="Hidden">
            <Button.Background>
                <LinearGradientBrush EndPoint="0,1" StartPoint="0,0">
                    <GradientStop Color="#FFF3F3F3" Offset="0"/>
                    <GradientStop Color="#FFEBEBEB" Offset="0.5"/>
                    <GradientStop Color="#FFDDDDDD" Offset="0.5"/>
                    <GradientStop Color="#FFCDCDCD" Offset="1"/>
                </LinearGradientBrush>
            </Button.Background>
        </Button>
        <TextBox x:Name="textboxSamAccountName"
HorizontalAlignment="Left" Margin="226,145,0,0"
TextWrapping="Wrap" VerticalAlignment="Top" Width="208"
TabIndex="5" MaxLength="20" Height="29" FontSize="14"/>
        <TextBox x:Name="textboxAdminUsername"
HorizontalAlignment="Left" Height="22" Margin="124,44,0,0"
TextWrapping="Wrap" VerticalAlignment="Top" Width="153"
TabIndex="1" Text="empresa\user" Visibility="Hidden"/>
        <PasswordBox x:Name="passwordboxAdminPassword"
HorizontalAlignment="Left" Height="22" Margin="124,77,0,0"
VerticalAlignment="Top" Width="153" TabIndex="2"
Password="xxxxxxxx" Visibility="Hidden"/>

```

```

    <Label Content="Admin User:" HorizontalAlignment="Left"
Margin="40,42,0,0" VerticalAlignment="Top" Width="75"
Visibility="Hidden"/>
    <Label Content="Admin Pass:" HorizontalAlignment="Left"
Margin="40,75,0,0" VerticalAlignment="Top" Width="75"
Visibility="Hidden"/>
    <Label Content="Contraseña Anterior: "
HorizontalAlignment="Left" Margin="226,196,0,0"
VerticalAlignment="Top" Width="144" FontSize="14"/>
    <Label Content="Nueva Contraseña:"
HorizontalAlignment="Left" Margin="226,271,0,0"
VerticalAlignment="Top" Width="135" FontSize="14"/>
    <TextBox x:Name="textboxOu" HorizontalAlignment="Left"
Height="33" Margin="74,108,0,0" TextWrapping="Wrap"
Text="TextBox" VerticalAlignment="Top" Width="295"
FontSize="10" TabIndex="3" Visibility="Hidden"/>
    <Label Content="Directory: " HorizontalAlignment="Left"
Margin="10,108,0,0" VerticalAlignment="Top"
Visibility="Hidden"/>
    <Label Content="Cuenta de Usuario: "
HorizontalAlignment="Left" Margin="226,115,0,0"
VerticalAlignment="Top" Width="135" FontSize="14"/>
    <PasswordBox x:Name="passwordboxUserPass"
HorizontalAlignment="Left" Height="29" Margin="226,300,0,0"
VerticalAlignment="Top" Width="143" TabIndex="6"
MaxLength="8" FontSize="14"/>
    <Label Content="Confirmar Contraseña:"
HorizontalAlignment="Left" Margin="226,348,0,0"
VerticalAlignment="Top" Width="154" FontSize="14"/>
    <Image HorizontalAlignment="Left" Height="77"
Margin="13,11,0,0" VerticalAlignment="Top" Width="193"
Source="D:\proyjava\utils-cambio-
passwd\ejecutables\AD\image\LogoSima.jpg"/>
    <PasswordBox x:Name="passwordboxUserPass_Ant"
HorizontalAlignment="Left" Height="29" Margin="226,224,0,0"
VerticalAlignment="Top" Width="143" TabIndex="6"
MaxLength="8" FontSize="14"/>
    <Button x:Name="btCerrar" Content="Cerrar"
HorizontalAlignment="Left" Margin="407,451,0,0"
VerticalAlignment="Top" Width="109" Click="btCerrar_Click"
Height="43" FontSize="14"/>
    <Button x:Name="btClave" Content="Generar Clave"
HorizontalAlignment="Left" Margin="18,374,0,0"
VerticalAlignment="Top" Width="99" Foreground="#FF170101"
Click="btClave_Click" Visibility="Hidden">
    </Button>
    <PasswordBox x:Name="passwordboxUserPass1"
HorizontalAlignment="Left" Height="29" Margin="226,377,0,0"

```

```

VerticalAlignment="Top" Width="143" TabIndex="6"
MaxLength="8" FontSize="14"/>
  <RichTextBox HorizontalAlignment="Left" Height="153"
Margin="407,271,0,0" VerticalAlignment="Top" Width="158"
IsReadOnly="True" FontSize="14" Foreground="#FF0A13CF"
Visibility="Hidden">
  <FlowDocument>
    <Paragraph LineHeight="6">
      <Run Language="es-pe" Text="Requisitos mínimos de
contraseña:"/>
    </Paragraph>
    <Paragraph LineHeight="6">
      <Run Language="es-pe" Text="* 1 Mayúscula"/>
    </Paragraph>
    <Paragraph LineHeight="6">
      <Run Language="es-pe" Text="* 1 numero"/>
    </Paragraph>
    <Paragraph LineHeight="6">
      <Run Language="es-pe" Text="* No usar "/>
      <Run Language="es-pe" Text="nombre"/>
    </Paragraph>
    <Paragraph LineHeight="6">
      <Run Language="es-pe" Text="* 8 caracteres"/>
    </Paragraph>
  </FlowDocument>
</RichTextBox>
  <Button Content="Conectar Samba"
HorizontalAlignment="Left" Margin="166,565,0,0"
VerticalAlignment="Top" Width="136" Click="Button_Click"
Height="43" Visibility="Hidden"/>
  <Button Content="Conectar Scorreo"
HorizontalAlignment="Left" Margin="304,567,0,0"
VerticalAlignment="Top" Width="136" Click="BtnCorreo_Click"
Height="43" Visibility="Hidden"/>
  <Button Content="Button" HorizontalAlignment="Left"
Margin="445,567,0,0" VerticalAlignment="Top" Width="75"
Click="Button_Click_1" Visibility="Hidden"/>
  <Button Content="Guardar" HorizontalAlignment="Left"
Margin="226,447,0,0" VerticalAlignment="Top" Width="122"
Height="47" Click="Button_Click_2" FontSize="14"/>
  <Button Content="Limpiar" HorizontalAlignment="Left"
Margin="208,481,0,0" VerticalAlignment="Top" Width="122"
Height="47" Click="Button_Click_3" Visibility="Hidden"/>
  <Image HorizontalAlignment="Left" Height="192"
Margin="13,137,0,0" VerticalAlignment="Top" Width="193"
Source="D:\projjava\utils-cambio-
passwd\ejecutables\AD\image\login.jpg"/>

```

```

        <Label Content="Copyright ©2018. Jmartinez"
HorizontalAlignment="Left" Height="31" Margin="407,601,0,0"
VerticalAlignment="Top" Width="186" FontSize="11"/>
        <Label Content="Copyright ©2018. Jmartinez"
HorizontalAlignment="Left" Height="35" Margin="414,526,0,0"
VerticalAlignment="Top" Width="181" FontSize="12"/>

    </Grid>
</Window>

```

////////////////////////////////////

Modulo Reportes

```

using System;
using System.Collections.Generic;
using System.Data;
using System.Data.SqlClient;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows;
using System.Windows.Controls;
using System.Windows.Data;
using System.Windows.Documents;
using System.Windows.Input;
using System.Windows.Media;
using System.Windows.Media.Imaging;
using System.Windows.Navigation;
using System.Windows.Shapes;

namespace AdReportes
{
    public partial class MainWindow : Window
    {
        public MainWindow()
        {
            InitializeComponent();
        }
        private void Button_Click(object sender, RoutedEventArgs e)
        {
            //Buscar
        }

        private void Button_Click_1(object sender, RoutedEventArgs e)
        {
            DataTable _dataTable = new DataTable();

```

```

        _dataTable = getrpt1();

        grid_rpt1.AutoGenerateColumns = true;
        grid_rpt1.ItemsSource = _dataTable.DefaultView;
    }

    //metodo que realiza la consulta
    public DataTable getrpt1() {

        DataTable _dataTable = new DataTable();
        SqlDataAdapter _adapter = new SqlDataAdapter();
        SqlDataReader _dr = new SqlDataReader();

        SqlConnection sqlCon = new SqlConnection(@"Data
Source=.; Initial Catalog=BDPASSW; Integrated Security=True;");
        try
        {
            if (sqlCon.State == ConnectionState.Closed)
                sqlCon.Open();
            String query = "SELECT saMacountname, pwdlastset1,
area, mail, fecMail, lastset FROM userpassw WHERE area=@area
AND usuario=@usuario";
            SqlCommand sqlCmd = new SqlCommand(query, sqlCon);
            sqlCmd.CommandType = CommandType.Text;
            sqlCmd.Parameters.AddWithValue("@area", txtArea.Text);
            sqlCmd.Parameters.AddWithValue("@usuario",
txtUsuario.Text);
            _adapter.SelectCommand = sqlCmd;
            _dr = sqlCmd.ExecuteReader();

            _dataTable.Load(_dr);
        }
        catch (Exception ex)
        {
            MessageBox.Show(ex.Message);
        }
        finally
        {
            sqlCon.Close();
        }

        return _dataTable;
    }
}
}
}
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

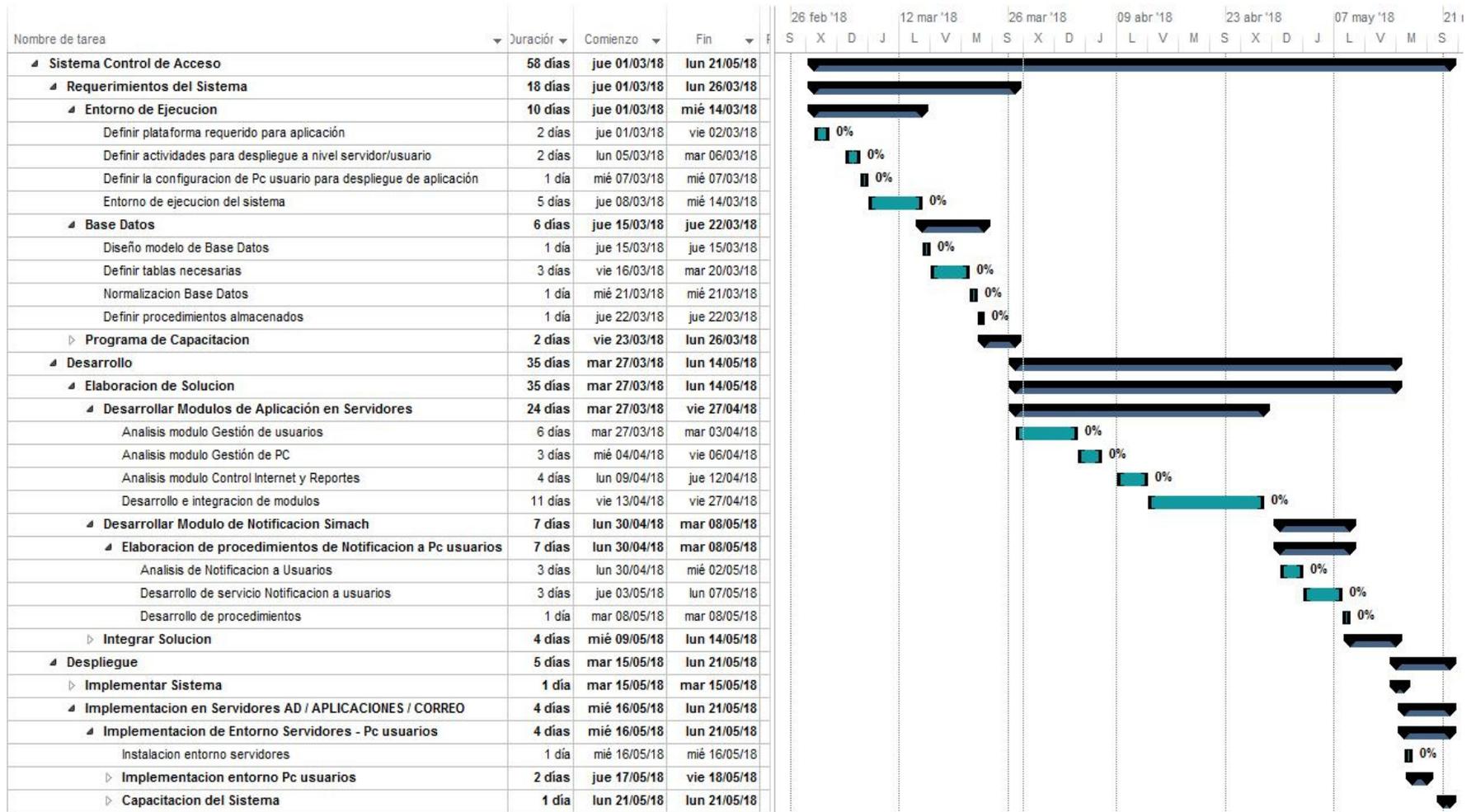
```

Tabla Nro. 54: Presupuesto implementación del sistema de control.

Ítem	Descripción	Cantidad	Costo unitario S/.	Total S/.
Proyecto	Jefe proyecto	1	3500.00	3500.00
Proyecto	Analista / programador	1	3000.00	3000.00
Base datos	SQL Server 2014	1	1700.00	1700.00
Software de desarrollo	Licencia Visual Studio 2013	1	1300.00	1300.00
Servidor	Se usará el servidor de aplicaciones existente en la empresa.	1	-----	-----
Laptop de pruebas	Lenovo Core i5 2.66 GHZ 8 GB ram, DD 1 TB	1	1500.00	1500.00
USB	Kingston 32 GB	1	30.00	30.00
			TOTAL	10,530.00

Fuente: Elaboración propia.

Gráfico Nro. 51: Cronograma implementación del sistema.



Fuente: Elaboración propia.

VI. CONCLUSIONES

De acuerdo a los resultados obtenidos, los que fueron analizados e interpretados, se llega a la conclusión que hay la necesidad de implementar el sistema de control que cubra las expectativas de la empresa debido al nivel de insatisfacción de los usuarios. Cabe indicar que esta interpretación coincide con lo propuesto en la hipótesis general de esta investigación planteando que la implementación del sistema de control de acceso a red en la empresa SIMA – Chimbote; 2018, mejora el control de cuentas de usuarios y la seguridad de la red. Por lo expuesto concluimos que la hipótesis general queda aceptada.

Así también llegamos a las siguientes conclusiones específicas:

1. En esta investigación se logró realizar la evaluación tecnológica lo cual permitió establecer los requisitos mínimos de hardware y software para el adecuado diseño del sistema de control de acceso de usuarios a red de la empresa SIMA - Chimbote.
2. Se evaluó las configuraciones existentes en los servidores Active Directory, Linux y Windows, que ayudó a establecer el alcance y limitaciones del sistema propuesto.
3. Se evaluó el entorno de desarrollo más conveniente, lo que ayudó a generar mayores prestaciones del sistema propuesto.
4. Se cumplió con la implementación del sistema de control lo cual mejoró el control de cuentas de usuarios y la seguridad de la red en la empresa SIMA – Chimbote.

VII. RECOMENDACIONES

1. Se sugiere que el jefe del área de tecnologías de la información y comunicaciones de la empresa disponga capacitaciones a los usuarios para una adecuada interacción con el sistema de control de acceso a red.
2. Se sugiere que el gerente de la empresa disponga la aprobación y difusión de las políticas de seguridad de red a los usuarios a fin de involucrarlos progresivamente en el manejo a nivel de terminales de usuarios.
3. Se sugiere que el jefe del área de tecnologías de la información y comunicaciones proponga al gerente de la empresa el despliegue del sistema de control de acceso a red.
4. Se sugiere que el gerente de la empresa incluya en su presupuesto económico la partida necesaria para el despliegue del sistema de control de acceso a red.

REFERENCIAS BIBLIOGRÁFICAS

1. Axelos. ITIL V3. 2014. Fundamentos ITIL V3.
2. INDECOPI. NTP-ISO/IEC 27001:2014. 2014. Norma Técnica Peruana. Tecnología de la Información. Técnicas de seguridad.
3. SGS.PE. Sgs. [Online].; 2017 [cited 2018 febrero 08. Available from: <http://www.sgs.pe/>.
4. World BASC Organization. World BASC Organization. [Online].; 2017 [cited 2018 febrero 08. Available from: <https://www.wbasco.org/espanol/normas.htm>.
5. Balsero Meneses AJ, Vargas Garcia CG. Implementación de un Prototipo para el Control de Acceso en la Sede de Ingeniería. Tesis pre-grado. Bogota - Colombia: Universidad Distrital Francisco José Caldas, Facultad de Ingeniería; 2016.
6. Ahumada Opicci DF. Sistema de Control de Acceso para un Endpoint. Tesis pre-grado. Santiago de Chile: Universidad De Chile, Ciencias De La Computación; 2015.
7. Cano Moreno JLA. Implementación del Sistema Centralizado de Autenticación y Autorización para las Aplicaciones Web del Centro de Cálculo e Investigación de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala. Tesis pre-grado. Guatemala: Universidad de San Carlos de Guatemala, Escuela de Ingeniería en Ciencias y Sistemas; 2014.
8. Blas Rinza JF. Seguridad y Control Del Acceso a las Redes Inalámbricas en la Unsm-T Mediante Servidores de Autenticación Radius con el Uso de Certificados Digitales. Tesis pre-grado. Tarapoto, Perú: Universidad Nacional De San Martín - T, Ingeniería de Sistemas e Informática; 2017.
9. Rivas Arellano MAM. Implementación De Un Sistema De Control De Acceso. Tesis pre-grado. Lima: Universidad Nacional Mayor De San Marcos, Facultad De Ingeniería De Sistemas E Informática; 2016.
10. Díaz Díaz JA, Salcedo Salazar JD. Sistema De Prevención De Intrusos Para Mejorar La Seguridad De Los Servidores De La Universidad Nacional De Trujillo. Tesis pre-grado. Trujillo, Perú: Universidad Nacional De Trujillo,

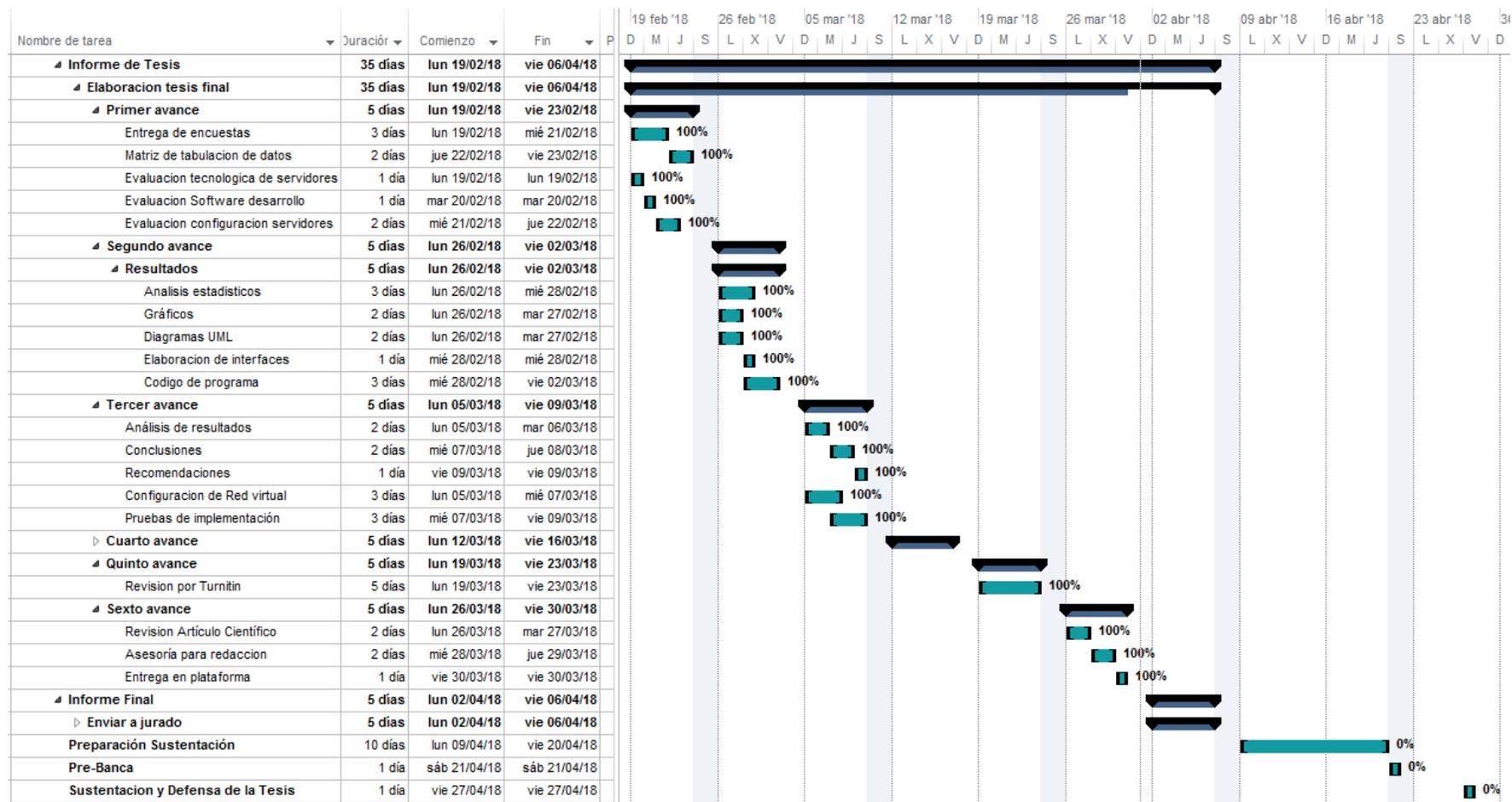
- Escuela Académico-Profesional De Informática; 2014.
11. Zuñiga Llamoca MA, Guevara Andrade LF. Diseño E Implementacion De Un Sistema En Plataforma Web Y Android Para Control De Acceso En La Empresa Minera Antapaccay. Tesis pre-grado. Arequipa: Universidad Tecnológica del Perú, Ingeniería de Sistemas e Informática; 2017.
 12. Alfaro Díaz MÁ. Sistema de Autenticación por Huella Digital para la Generación de Reportes Sobre el Recurso Humano de la Institución Educativa Los Sauces. Tesis pre-grado. Trujillo: Universidad Privada Antenor Orrego, Escuela de Ingeniería de Computación y Sistemas; 2016.
 13. Candia Aguilar MP, Chavez Zuñiga DI. Sistema que Permite el Control de Accesos y el Uso de Recursos de los Usuarios en la Biblioteca Virtual de La Universidad Católica de Santa María Aplicando la Metodología de Desarrollo Extreme Programming. Tesis pre-grado. Arequipa: Universidad Catolica De Santa Maria, Escuela Profesional De Ingenieria De Sistemas; 2015.
 14. Centrum Graduate Business School PUCP. El Nuevo Entorno de la Economía Mundial. *Strategia*. 2016 Setiembre; 10(42): p. 140 - 160.
 15. SIMA Peru: SIMA-Chimbote. Servicios Industriales de la Marina S.A SIMA-Chimbote. [Online].; 2018 [cited 2018 febrero 09. Available from: <http://www.sima.com.pe/>.
 16. Tasa. Tasa. [Online].; 2018 [cited 2018 febrero 27-02-2018. Available from: <http://www.tasa.com.pe/nuestra-empresa/unidades-de-negocio/astillero.html#a>.
 17. Construcciones A. Maggiolo S.A. Construcciones A. Maggiolo S.A. [Online].; 2018 [cited 2018 febrero 27. Available from: <http://www.maggiolo.com.pe/es/quienes-somos>.
 18. Google. Google Maps. [Online].; 2018 [cited 2018 febrero 16. Available from: https://www.google.com.pe/search?q=sima+chimbote&npsic=0&rflfq=1&rlha=0&rllag=-9097393,-78579939,3835&tbm=lcl&ved=0ahUKEwiYxYzhvavZAhWIXFkKHW3oDhEQtgMIJw&tbs=lr:!2m1!1e2!3sIAE,lf:1,lf_ui:2&rldoc=1#rffi=hd;;si;;mv:!1m3!1d5693.881350436308!2d-78.5583152650.
 19. CONCYTEC. Programa Nacional Transversal De Tecnologías De La

- Información Y Comunicación 2016 - 2021 Lima: Biblioteca Nacional del Perú; 2016.
20. TECNOSEGURO. Tecnoseguro. [Online].; 2018 [cited 2018 febrero 09. Available from: <https://www.tecnoseguro.com>.
 21. ALEGSA. Diccionario de Informatica y Tecnología. [Online].; 2017 [cited 2018 febrero 09. Available from: <http://www.alegsa.com.ar/Dic>.
 22. Von Bertalanffy L. Teoria general de los sistemas. Fundamentos, desarrollo, aplicaciones Mexico: Fondo de cultura económica; 1976.
 23. Colobran Huguet M, Arqués Soldevilla JM, Eduard MG. Administración de sistemas operativos en red Barcelona: Editorial UOC; 2008.
 24. Definicion ABC. Definicion Abc Tu Diccionario Fácil. [Online].; 2017 [cited 2018 febrero 09. Available from: <https://www.definicionabc.com/tecnologia/informacion.php>.
 25. Vega JÁ. El gran libro de Windows Server 2008. Primera edición ed. México: Alfaomega; 2009.
 26. Barrios Dueñas J. Configuración De servidores Con GNU/Linux México: Alcance Libre; 2017.
 27. ISACA. Isaca. [Online].; 2018 [cited 2018 febrero 09. Available from: <https://www.isaca.org/>.
 28. ESET. Welivesecurity. [Online].; 2011 [cited 2018 febrero 09. Available from: <https://www.welivesecurity.com/la-es/2011/05/11/controles-seguridad-empresa/>.
 29. Roa Buendía JF. Seguridad informática España: McGraw-Hill; 2013.
 30. Borghello C. SEGU-INFO Seguridad de la Información. [Online].; 2017 [cited 2018 febrero 09. Available from: <https://www.segu-info.com.ar/logica/seguridadlogica.htm>.
 31. Gómez Vieites Á. Seguridad en equipos informáticos Central PE, editor. Madrid: RA-MA Editorial; 2014.
 32. Laudon K. Administración De Los Sistemas De Información: Organización Y Tecnología. 3rd ed. Mexico: Prentice Hall Hispanoamericana S.A; 1997.

33. Sommerville I. Ingeniería del Software. 7th ed. Martin-Romo M, editor. Madrid: Pearson Education; 2005.
34. Russel C, Zacker C. Introducing Windows Server 2008 R2 Press M, editor. Washington - EE.UU: nSight Inc.; 2010.
35. Ricardo CM. Bases de datos. primera edición ed. México: McGraw-Hill; 2009.
36. Guérin BA. ASP.NET 4.5 en C# con Visual Studio 2012 Mexico: Ediciones ENI; 2013.
37. Landa Cosio NA. C# Guía total del programador. 1st ed. Buenos Aires: Fox Andina; 2010.
38. Hernández Sampieri R. Metodología De La Investigación. sexta ed. México: Mc Graw Hill; 2014.
39. Sandoval R. LinkedIn. [Online].; 2016 [cited 2018 febrero 09. Available from: <https://es.linkedin.com/pulse/para-que-sirve-un-sistema-de-control-acceso-rovillel-sandoval>.

ANEXOS

ANEXO NRO. 1: CRONOGRAMA DE ACTIVIDADES



Fuente: Elaboración propia.

ANEXO NRO. 2: PRESUPUESTO

TITULO: Implementación de un Sistema de Control de Acceso a Red en la Empresa SIMA - Chimbote; 2018.

TESISTA: Jehu Benigno Martinez Cabrera

INVERSIÓN: S/. 4,270.00

FINANCIAMIENTO: recursos propios.

Rubro	Descripción	Cantidad	Costo unitario S/.	Total S/.
Material escritorio	Papel bond a-4 80gr (x1000)	1000	0.06	60.00
Sistema operativo	Ms Windows 7	1	250.00	250.00
Software de desarrollo	Visual Studio 2013	1	1300.00	1300.00
Computadora	Core i7 2.66 GHZ 8 GB ram, DD 500 GB, monitor 24'', teclado y mouse	1	950.00	950.00
Laptop	Lenovo Core i5 2.66 GHZ 8 GB ram, DD 1 TB	1	1500.00	1500.00
USB	Kingston 32 GB	1	30.00	30.00
Impresora	HP Multifuncional	1	180.00	180.00
			TOTAL	4270.00

Fuente: Elaboración Propia

ANEXO NRO. 3: CUESTIONARIO

TITULO: Implementación de un sistema de control de acceso a red en la empresa SIMA - Chimbote; 2018.

TESISTA: Jehu Benigno Martinez Cabrera

PRESENTACIÓN:

El presente instrumento forma parte del actual trabajo de investigación; por lo que se solicita su participación, respondiendo a cada pregunta de manera objetiva y veraz. La información a proporcionar es de carácter confidencial y reservado; y los resultados de la misma serán utilizados solo para efectos académicos y de investigación científica.

INSTRUCCIONES:

A continuación, se le presenta una lista de preguntas, agrupadas por dimensión, que se solicita se responda, marcando una sola alternativa con un aspa (“X”) en el recuadro correspondiente (SI o NO) según considere su alternativa, ver el siguiente ejemplo:

NRO.	PREGUNTA	SI	NO
1	¿Se siente satisfecho por la atención referente a sus cuentas de acceso?	X	

DIMENSIÓN 1: NIVEL DE SATISFACCIÓN DEL ACTUAL CONTROL DE ACCESO A RED			
NRO.	PREGUNTA	SI	NO
1	¿Se siente satisfecho por la atención referente a sus cuentas de acceso?		
2	¿Puede compartir recursos de la PC asignada?		
3	¿Tiene acceso a puertos USB?		
4	¿Puede instalar software en la PC asignada?		
5	¿Hay acceso a internet sin restricciones?		
6	¿Existen políticas de acceso a internet?		
7	¿Se cambia la contraseña de usuario luego de una reasignación de puesto?		
8	¿Se realiza la cancelación de privilegios en todos los servidores a los usuarios que dejan de laborar en la empresa?		
9	¿Se registran los incidentes relacionados con accesos a red?		
10	¿Se tiene herramientas y/o configuraciones para identificar automáticamente a los equipos que se conectan a la red?		
DIMENSIÓN 2: NECESIDAD DE PROPUESTA PARA EL CONTROL DE ACCESO POR MEDIO DE UN SISTEMA.			
NRO.	PREGUNTA	SI	NO

1	¿Cree que la implementación de un sistema de control mejorará el control de accesos de usuarios a red?		
2	¿Cree que es necesario que el sistema propuesto sea amigable de usar para el administrador y permita procesar las tareas en menor tiempo?		
3	¿Cree usted que hay funciones que requieren incorporarse en el sistema de control propuesto?		
4	¿Cree que el actual proceso de control de accesos debe mejorar?		
5	¿Es necesario que el sistema propuesto considere funciones centralizadas en mayor medida que los actuales?		
6	¿Cree que es necesario que el sistema propuesto considere reportes ágiles, fáciles de acceder y posibiliten que el Jefe TI haga seguimiento?		
7	¿Cree que la implementación del nuevo sistema dará mayor funcionalidad y seguridad en el control de accesos a red?		
8	¿Cree que debe mejorarse la eficiencia del control de accesos?		
9	¿Cree que el sistema propuesto debe permitir que el mismo usuario cambie periódicamente su contraseña de acceso a red de acuerdo a las políticas de la empresa?		
10	¿Cree que el usuario debe ser notificado vía correo con antelación a la caducidad de su contraseña de red?		