UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Aplicación de Reconocimiento Biométrico por Huella Dactilar y su Influencia en la Seguridad Lógica en SEDAPAL, 2020.

TESIS PARA OBTENER EL TÍTULO PROFESISONAL DE INGENIERO DE SISTEMAS

AUTORES:

Guerra Jiménez, Gustavo Mauricio (ORCID: 0000-0001-9714-7532)

Jiménez Prada, Ricardo Antonio (ORCID: 0000-0003-2487-6456)

ASESOR:

Dr. Chumpe Agesto, Juan Brues Lee (ORCID: 0000-0001-7466-9872)

LINEA DE INVESTIGACIÓN:

Sistema de Información y Comunicaciones

CALLAO – PERÚ

2021

Dedicatoria

El presente proyecto de investigación está dedicado a nuestros Padres, impulsores de nuestros logros y a aquellas personas que nos brindaron su apoyo para seguir adelante con el objetivo de cumplir nuestras metas personales y profesionales.

LOS AUTORES

Agradecimiento

A la Universidad César Vallejo, por habernos brindarnos la oportunidad de alcanzar nuestra meta profesional, a través del Equipo de Investigación, quienes pusieron a disposición los recursos necesarios.

LOS AUTORES

Página del jurado

Declaración de autenticidad

Índice de contenidos

Caratula i
Dedicatoria ii
Agradecimiento iii
Página del jurado iv
Declaración de autenticidad v
Índice de contenidos vi
Índice de tablas ix
Índice de gráficos y figuras xii
Resumen xiv
Abstract xv
I. INTRODUCCIÓN 16
1.1. Realidad Problemática 17
1.2. Formulación del problema 23
1.2.1. General 23
1.2.2. Específicos 23
1.3. Justificación 23
1.3.1. Institucional 23
1.3.2. Operativo 24
1.3.3. Tecnológico 24
1.3.4. Económico 25
1.4. Objetivos 25
1.4.1. General 25
1.4.2. Específicos 25
1.5. Hipótesis 26
1.5.1. General 26
1.5.2. Específicos 26
II. MARCO TEÓRICO 27
2.1. Antecedentes 28
2.1.1. Antecedentes Nacionales 28

2.1.2. Antecedentes Internacionales 31
2.2. Bases Teóricas 34
2.2.1. Bases teóricas de la variable independiente 34
2.2.2. Bases teóricas de la variable dependiente 46
III. METODOLOGÍA 76
3.1. Tipo, nivel y diseño de investigación 77
3.1.1. Variables y operacionalización 77
3.1.2. Población (criterios de selección), muestra, muestreo, unicidad de análisis . 79
3.2. Técnicas e instrumentos de recolección de datos 79
3.3. Procedimientos 80
3.4. Método de análisis de datos 81
3.5. Aspectos éticos 82
IV. RESULTADOS 83
4.1. Descripción y análisis estadístico 84
4.1.1. Pre prueba de la variable dependiente: Seguridad Lógica 84
4.1.2. Post prueba de la variable dependiente: Seguridad Lógica 99
4.2. Contrastación de hipótesis 115
4.2.1. Hipótesis principal 115
4.2.2. Hipótesis secundarias 120
V. DISCUSIÓN 132
VI. CONCLUSIONES 138
VII. RECOMENDACIONES 141
VIII. REFERENCIAS 143
IX. ANEXOS 149
Anexo 1: Matriz de Consistencia 150
Anexo 2: Matriz de Operacionalización de la Variable Dependiente 151
Anexo 3: Instrumento 152
Anexo 4: Validación del Instrumento 154
Anexo 5: Matriz de Datos 160
Anexo 6: Solicitud de Aplicación de encuesta. 162
Anexo 7: Carta de autorización de aplicación de encuesta. 163

Anexo 8: Informe Técnico 164

Índice de tablas

Tabla 01: Operacionalización de la Variable Dependiente 78
Tabla 02: Ficha Técnica de recolección de datos 80
Tabla 03: Estadística de fiabilidad 81
Tabla 04: Pre Prueba - No resulta tedioso a los usuarios ingresar las credenciales de acceso a los programas informáticos. 84
Tabla 05: Pre Prueba - El tiempo para el proceso de autenticación es óptimo. 85
Tabla 06: Pre Prueba - La autenticación de usuarios a los programas informáticos es segura 86
Tabla 07: Pre Prueba - El proceso de autenticación permite el acceso a una cuenta solo a la persona autorizada. 87
Tabla 08: Pre Prueba - Las credenciales de acceso de los usuarios no tienden a ser olvidadas. 88
Tabla 09: Pre Prueba - La cantidad de credenciales asignadas a los usuarios para acceder a los programas informáticos es adecuado 89
Tabla 10: Pre Prueba - El descuido del usuario no representa una amenaza para el proceso de autenticación. 90
Tabla 11: Pre Prueba - El espionaje corporativo no es una amenaza difícil de detectar en el proceso de autenticación de usuarios. 91
Tabla 12: Pre Prueba - El proceso de autenticación es propenso a un ataque por manipulación de personas. 92
Tabla 13: Pre Prueba - El proceso de autenticación limita a los usuarios compartir sus credenciales con otras personas. 93
Tabla 14: Pre Prueba - La cooperación consiente de un usuario en un ataque informático que no afecta el proceso de autenticación. 94
Tabla 15: Pre Prueba - El proceso de autenticación permite asegurar la identidad veraz de una persona asociado a la cuenta con la que accedió. 95
Tabla 16: Pre Prueba El proceso de autenticación permite llevar un registro de actividad confiable de los usuarios dentro del sistema. 96
Tabla 17: Pre Prueba - El proceso de autenticación de usuarios permite minimizar la ruptura de credenciales de acceso. 97
Tabla 18: Pre Prueba - La autenticación de usuarios no está sujeto al robo de credenciales. 98

Tabla 19: Post Prueba - No resulta tedioso a los usuarios ingresar las credenciales de acceso a los programas informáticos. 100
Tabla 20: Post Prueba - El tiempo para el proceso de autenticación es óptimo. 101
Tabla 21; Post Prueba - La autenticación de usuarios a los programas informáticos es segura. 102
Tabla 22: Post Prueba - El proceso de autenticación permite el acceso a una cuenta solo a la persona autorizada. 103
Tabla 23: Post Prueba - Las credenciales de acceso de los usuarios no tienden a ser olvidadas 104
Tabla 24: Post Prueba - La cantidad de credenciales asignadas a los usuarios para acceder a los programas informáticos es adecuado. 105
Tabla 25: Post Prueba - El descuido del usuario no representa una amenaza para el proceso de autenticación 106
Tabla 26: Post Prueba - El espionaje corporativo no es una amenaza difícil de detectar en el proceso de autenticación de usuarios. 107
Tabla 27: Post Prueba - El proceso de autenticación es propenso a un ataque por manipulación de personas. 108
Tabla 28: Post Prueba - El proceso de autenticación limita a los usuarios compartir sus credenciales con otras personas. 109
Tabla 29: Post Prueba - La cooperación consiente de un usuario en un ataque informático que no afecta el proceso de autenticación. 110
Tabla 30: Post Prueba - El proceso de autenticación permite asegurar la identidad veraz de una persona asociado a la cuenta con la que accedió. 111
Tabla 31: Post Prueba El proceso de autenticación permite llevar un registro de actividad confiable de los usuarios dentro del sistema. 112
Tabla 32: Post Prueba - El proceso de autenticación de usuarios permite minimizar la ruptura de credenciales de acceso. 113
Tabla 33: Post Prueba - La autenticación de usuarios no está sujeto al robo de credenciales. 114
Tabla 34: Estadísticos de tendencia central - Pre Prueba 115
Tabla 35: Datos de frecuencia - Pre Prueba 116
Tabla 36: Datos de frecuencia – Post Prueba 117
Tabla 37: Contrastación hipótesis principal 118

Tabla 38: Estadísticos de Prueba - Hipótesis principal.....119
Tabla 39: Estadísticos de tendencia central – Primera dimensión. 120
Tabla 40: Datos de frecuencia - Pre Prueba primera dimensión. 120
Tabla 41: Datos de frecuencia - Post Prueba primera dimensión.....121
Tabla 42: Estadísticos de prueba –Hipótesis secundaria 1 123
Tabla 43: Estadísticos de tendencia central - Segunda dimensión.....124
Tabla 44: Datos de frecuencia - Pre Prueba segunda dimensión.....124
Tabla 45: Datos de frecuencia - Post Prueba segunda dimensión. 124
Tabla 46: Estadísticos de prueba –Hipótesis secundaria 2 126
Tabla 47: Estadísticos de tendencia central - Tercera dimensión. 127
Tabla 48: Datos de frecuencia - Pre Prueba tercera dimensión. 128
Tabla 49: Datos de frecuencia - Post Prueba tercera dimensión.....128
Tabla 50: Estadísticos de prueba –Hipótesis secundaria 3 130

Índice de gráficos y figuras

Figura 01: Pre Prueba - No resulta tedioso a los usuarios ingresar las credenciales de acceso a los programas informáticos. 85
Figura 02. Pre Prueba - El tiempo para el proceso de autenticación es óptimo. 86
Figura 03. Pre Prueba - La autenticación de usuarios a los programas informáticos es segura. 87
Figura 04. Pre Prueba - El proceso de autenticación permite el acceso a una cuenta solo a la persona autorizada. 88
Figura 05. Pre Prueba - Las credenciales de acceso de los usuarios no tienden a ser olvidadas. 89
Figura 06. Pre Prueba - La cantidad de credenciales asignadas a los usuarios para acceder a los programas informáticos es adecuado. 90
Figura 07. Pre Prueba - El descuido del usuario no representa una amenaza para el proceso de autenticación. 91
Figura 08. Pre Prueba - El espionaje corporativo no es una amenaza difícil de detectar en el proceso de autenticación de usuarios. 92
Figura 09. Pre Prueba - El proceso de autenticación es propenso a un ataque por manipulación de personas. 93
Figura 10. Pre Prueba - El proceso de autenticación limita a los usuarios compartir sus credenciales con otras personas. 94
Figura 11. Pre Prueba - La cooperación consiente de un usuario en un ataque informático que no afecta el proceso de autenticación. 95
Figura 12. Pre Prueba - El proceso de autenticación permite asegurar la identidad veraz de una persona asociado a la cuenta con la que accedió. 96
Figura 13. Pre Prueba El proceso de autenticación permite llevar un registro de actividad confiable de los usuarios dentro del sistema. 97
Figura 14. Pre Prueba - El proceso de autenticación de usuarios permite minimizar la ruptura de credenciales de acceso. 98
Figura 15. Pre Prueba - La autenticación de usuarios no está sujeto al robo de credenciales. 99
Figura 16. Post Prueba - No resulta tedioso a los usuarios ingresar las credenciales de acceso a los programas informáticos. 100
Figura 17. Post Prueba - El tiempo para el proceso de autenticación es óptimo. 101

Figura 18. Post Prueba - La autenticación de usuarios a los programas informáticos es segura. 102
Figura 19. Post Prueba - El proceso de autenticación permite el acceso a una cuenta solo a la persona autorizada. 103
Figura 20. Post Prueba - Las credenciales de acceso de los usuarios no tienden a ser olvidadas. 104
Figura 21. Post Prueba - La cantidad de credenciales asignadas a los usuarios para acceder a los programas informáticos es adecuado. 105
Figura 22. Post Prueba - El descuido del usuario no representa una amenaza para el proceso de autenticación. 106
Figura 23. Post Prueba - El espionaje corporativo no es una amenaza difícil de detectar en el proceso de autenticación de usuarios. 107
Figura 24. Post Prueba - El proceso de autenticación es propenso a un ataque por manipulación de personas. 108
Figura 25. Post Prueba - El proceso de autenticación limita a los usuarios compartir sus credenciales con otras personas. 109
Figura 26. Post Prueba - La cooperación consiente de un usuario en un ataque informático que no afecta el proceso de autenticación. 110
Figura 27. Post Prueba - El proceso de autenticación permite asegurar la identidad veraz de una persona asociado a la cuenta con la que accedió. 111
Figura 28. Post Prueba El proceso de autenticación permite llevar un registro de actividad confiable de los usuarios dentro del sistema. 112
Figura 29. Post Prueba - El proceso de autenticación de usuarios permite minimizar la ruptura de credenciales de acceso. 113
Figura 30. Post Prueba - La autenticación de usuarios no está sujeto al robo de credenciales. 114
Figura 31. Datos de frecuencia - Pre Prueba. 116
Figura 32. Datos de frecuencia - Post Prueba. 118
Figura 33. Datos de frecuencia - Pre Prueba primera dimensión. 122
Figura 34. Datos de frecuencia - Post Prueba primera dimensión. 122
Figura 35. Datos de frecuencia – Pre prueba segunda dimensión. 125
Figura 36. Datos de frecuencia – Post prueba segunda dimensión 126
Figura 38. Datos de frecuencia – Post prueba tercera dimensión. 130

Resumen

El objetivo general es determinar de qué manera influye la aplicación de reconocimiento biométrico por huella dactilar en la seguridad lógica, teniendo una población de estudio de 52 trabajadores del área comercial de SEDAPAL, de la cual se obtuvo una muestra censal. Además, se utilizó el diseño de investigación Experimental del tipo Pre-Experimental empleando el método de estudio del Pre Test y Post Test, se utilizó la prueba de rangos con signos de Wilcoxon, con el fin de determinar el rango medio de dos muestras relacionadas y comprobar si existen diferencias entre ellas. Se concluyó que en la pre prueba se obtuvo una media de 30.51, asimismo, en la post prueba se obtuvo una media de 53.19, lo que significa que resultó en un incremento del 74. 33 % en referencia a la influencia del reconocimiento biométrico por huella dactilar en la seguridad lógica. De la misma manera, para la dimensión control de acceso se alcanzó una media de 11.98 en la pre prueba, en contraste con la media de la post prueba, la cual resultó con una media de 21.42 constituyendo un incremento del 78.79 % de influencia del reconocimiento biométrico por huella dactilar. Por otro lado, para la dimensión ingeniería social se alcanzó una media de 10.46 en la pre prueba, a diferencia de la media de la post prueba, la cual obtuvo una media de 17.19, incrementando un 64.34 % referido a la influencia del reconocimiento biométrico por huella dactilar en la ingeniería social. Finalmente, para la dimensión auditoria de seguridad se logró una media de 14.57 en la pre prueba, a comparación con la media de la post prueba, la cual resulto con una media de 8.03, observándose un incremento del 81.44 % conforme a la influencia del reconocimiento biométrico por huella dactilar.

Palabras Claves: Reconocimiento biométrico por huella dactilar, seguridad lógica.

Abstract

The general objective is to determine how the application of biometric fingerprint recognition influences logical security, the study population is 52 workers from the SEDAPAL commercial area, from which a census sample was obtained. In addition, the research design was experimental - Pre-Experimental using the Pre-Test and Post Test study method. The Wilcoxon signed rank test was used in order to determine the mean range of two related samples and check if there were differences between them. It is concluded that in the pre-test an average of 30.51 was obtained, likewise, in the post-test an average of 53.19 was obtained, which means that it resulted in an increase of 74. 33% in reference to the influence of biometric recognition by fingerprint in logical security. In the same way, for the access control dimension, the mean that was reached was 11.98 in the pre-test, in contrast to the post-test mean, which resulted with a mean of 21.42, constituting an increase of 78.79% of influence. of biometric fingerprint recognition. On the other hand, for the social engineering dimension, the mean obtained was 10.46 in the pre-test, unlike the mean of the post-test, which obtained an average of 17.19, increasing by 64.34% referring to the influence of biometric recognition by fingerprint in social engineering. Finally, for the security audit dimension, an average of 14.57 was achieved in the pre-test, compared to the average of the post-test, which resulted with an average of 8.03, observing an increase of 81.44% according to the influence of biometric recognition. by fingerprint.

Keywords: Biometric recognition by fingerprint, logical security.

I. INTRODUCCIÓN

1.1. Realidad Problemática

A nivel mundial, las tecnologías de la información han alcanzado un gran desarrollo en los últimos años, revolucionando el modo en que las organizaciones gestionan su modelo de negocio, adaptando sus necesidades a nuevas posibilidades tecnológicas. Según De Pablos et al. (2019) afirman que la eficacia de un sistema de información depende de la capacidad que posee para facilitar la información que la organización necesita en el momento oportuno, y su eficiencia por realizarlo utilizando el mínimo de recursos empresariales posibles.

De acuerdo a lo anterior, existe un gran enfoque de parte de las organizaciones por apoyar a las tecnologías de la información, caracterizados por ocupar un desarrollado conjunto de elementos imprescindibles para satisfacer las necesidades primarias de información. Córdova y Santana (2011) explican que las organizaciones se apoyan en las tecnologías de información para agilizar sus procesos y tomar decisiones más precisas contribuyendo en ventajas competitivas sostenibles.

Actualmente, una de las grandes preocupaciones para usuarios de la tecnología, es tener la certeza de que cada uno de los sistemas de información que disponen estén realmente seguros. De acuerdo con Silva et al. (2014) describe que la seguridad es necesaria para la estabilidad de las organizaciones independientemente de su estructura, debido a que permiten niveles de protección de la información, garantizando la integridad de estos para la toma de decisiones estratégicas.

Globalmente se trabaja en el desarrollo de nuevas formas que permitan reducir la incertidumbre relacionada a la seguridad de la información en un mundo interconectado, en especial cuando la misma es la fuente y base para un desarrollo óptimo de las diversas actividades que la complementan, incluso cuando se encuentra expuesta a usos inadecuados y carencias relacionadas con la protección de datos.

Según Aguilera (2011) un sistema de información, particularmente de las medidas de seguridad aplicadas, presentará un margen de riesgo existente. Asimismo, de acuerdo con Escrivá et al. (2013) para determinar la seguridad de un sistema, es necesario garantizar la disponibilidad, confidencialidad e integridad de la información.

Aunque de acuerdo con diversos estudios realizados por especialistas, no existe ningún sistema completamente seguro, se debe pretender proteger la información y el sistema que la proporciona, en virtud de brindar a los usuarios un grado de seguridad razonable. (Escrivá et al. 2013).

La seguridad debe complementarse en todos sus niveles y clasificaciones implícitos en los sistemas informáticos, por lo que su enfoque central debe preservarse a partir de mecanismos que garanticen su protección. De acuerdo con Aguilera (2011), define como núcleo a los mecanismos y servicios de protección a las propiedades relacionadas a la integridad, disponibilidad y confidencialidad referidas a los sistemas de información, de igual manera, según Escrivá et al. (2013) menciona que son técnicas que resguardan la función lógica de un sistema informático.

En la actualidad, existen diversas opciones complementarias a fortalecer los sistemas de seguridad de la información, es por ello que la utilización de más de un método aumenta las probabilidades de alcanzar el nivel adecuado de seguridad, sin embargo, esta afirmación no siempre converge a la solución definitiva, debido a que los mecanismos de autenticación tradicionales ya no garantizan la eficiencia de este campo. De acuerdo a Simón (2003), explica que, los métodos tradicionales no son fiables entre individuos legítimos e impostores, debido a que la identidad puede ser corrompida o en otros casos particulares al individuo, puede ser olvidada.

En esencia, unos de los caminos que se abre paso a revolucionar de una forma particular la seguridad lógica de los sistemas de información, es la tecnología biométrica, la cual se basa en un sistema de reconocimiento mediante la utilización de alguna parte del cuerpo o comportamiento específico. Simón (2003), afirma que proporcionan una mayor fiabilidad en la identidad de la persona, debido a que son intransferibles, permitiendo de esta manera acceder a nuevos niveles de seguridad y comodidad para los usuarios.

Diversas organizaciones recurren a dispositivos biométricos para controlar la autenticación, orientadas a proteger los datos inmersos en las actividades más cotidianas que involucran una alta importancia para la sostenibilidad futura de las

mismas. Un estudio de la Asociación de Examinadores de Fraude Certificados (2019), reveló que un progresivo número de organizaciones han implementado la tecnología biométrica y analítica de alto nivel en sus estrategias de gestión para la seguridad, asimismo, reveló que, en un gran porcentaje las organizaciones incorporan tecnologías biométricas, como lectores de huella dactilar, para aumentar la seguridad.

De esta manera, las herramientas biométricas ayudan a reducir significativamente los fraudes y el tiempo en los procesos administrativos inherentes a sus objetivos estratégicos. Los sistemas biométricos han demostrado ser uno de los instrumentos de seguridad más eficaces actualmente. Según un estudio de Virtual Instrument Software Architecture (2016), de acuerdo al estudio realizado en España se obtuvo como resultado que el 50% de los encuestados mostraron un gran interés por el uso de la biometría como mecanismo de autenticación, asimismo, se observó un incremento en la autenticación por huella dactilar con relación a la realización de transacciones a través de dispositivos móviles, considerándose como el método más seguro en la biometría.

Hoy en día, gran parte de la sociedad mantiene el enfoque, y parcialmente su respaldo con respecto a la seguridad de su información por medio de claves, tarjetas de acceso u otros medios tradicionales de autenticación; sin embargo, no evalúan el hecho de que esos métodos son potencialmente inseguros, es decir, cumplen su funcionalidad, pero pueden comprometerse a ser extraviados, robados, modificados, duplicados, entre otras casuísticas. Según Carri et. al (2007), explica que tecnologías como tarjetas de acceso o cualquier uso de contraseñas presentan vulnerabilidades en la seguridad, que pueden tener efectos negativos según la clase de aplicación en la que estén implicadas.

Por otro lado, se han acogido nuevos modelos operativos tecnológicos en las organizaciones, utilizado como medio transaccional para la información. Por tanto, la seguridad resulta ser un tema de primera línea para la gestión, y ante ello, el reconocimiento dactilar resulta ser la forma más práctica y segura para realizar transacciones. Instituto nacional de tecnologías y comunicaciones (2011) afirman que las ventajas se orientan en el aumento de la seguridad, la disminución de las

posibilidades de fraude, incremento de la usabilidad brindando comodidad por la sustitución de claves de acceso, como también, reforzamiento de la privacidad del usuario.

En América Latina, la utilización de la biometría para optimizar la seguridad, se encuentra respaldada por múltiples proyectos ya implementados en diferentes países, donde esta tecnología es utilizada por los cuerpos de seguridad para monitorear, controlar, identificar y prevenir los delitos. La última tendencia es el desarrollo de un sistema de identificación electrónica (e-ID) nacional. Muchos países de Latinoamérica aún no cuentan con la infraestructura necesaria para realizar una autenticación e identificación biométrica segura de los ciudadanos". (Yeliseyev, 2016).

Podemos decir que la identificación biométrica está siendo implementada de manera muy limitada en Latinoamérica, porque la mayoría de gobiernos, incluyendo empresas privadas, mantienen los procesos de identificación tradicionales. Según Banco Bilbao Vizcaya Argentaria (2016) independientemente de proponer erradicar el uso de contraseñas, se propone implementar un sistema de autenticación completo, que integre sistemas biométricos sin dejar de lado el uso de contraseñas, y partiendo de ello, optimizar algunos o muchos factores de dicho sistema, que entre los principales destaque: la seguridad, velocidad, utilidad, funcionalidad, facilidad de gestión, costos de mantenimiento, entre otros.

Según el Instituto Nacional de Tecnologías de la Comunicación (2011) más allá de la técnica utilizada, los sistemas biométricos son empleados en diferentes campos con múltiples fines. Los resultados obtenidos a partir de las entrevistas realizadas indican que, el principal objetivo de la biometría es el control de acceso de un individuo a un ambiente o infraestructura (real o virtual) tanto a nivel físico como lógico.

Pero la identificación biométrica debe ser implementada en una estructura gubernamental que asuma como tal esta tecnología y poder extraer todos los beneficios que puede ofrecer.

Las preocupaciones de los equipos de seguridad en las empresas pueden determinarse a través de distintos factores, como las tendencias en materia de

amenazas informáticas o los incidentes de seguridad más comunes. Según Kaspersky (2018) a pesar de la existencia real de riesgos, la biometría como tecnología sigue brindando fuertes soluciones de seguridad debido a su dificultad de replicación. Los sistemas biométricos resultan ser un gran reemplazo en lo que a nombres de usuarios respecta como miembro de una estrategia de autenticación de doble factor al poseer elementos propios, como rasgos físicos (biometría), de pertenecía (tokens de hardware) o para recordar (passwords).

La atención proactiva de estas inquietudes contribuye a evitar la materialización de los riesgos asociados a la seguridad de la información. De acuerdo a un estudio realizado por ESET Security (2016), la principal preocupación es las 'vulnerabilidades de software y sistemas', con el 58% de las respuestas afirmativas, seguido por el 'Malware' (54%) y, en el tercer puesto, el 'Acceso indebido la información' (46%). Si bien es cierto, el acceso indebido a la información está en último puesto según el reporte emitido por ESET Security, este viene a ser un problema interno para toda organización, pues es causado por los mismos colaboradores. La mala manipulación de la información se puede dar por múltiples causas, por ello es importante que se asuman políticas de manejo de la información para evitar este gran problema. Además de crear una conciencia ética y profesional entre los mismos colaboradores que tienen acceso directo a la información sensible, con el fin de que se concientice adecuadamente.

En el Perú, el Registro nacional de identificación y estado civil (RENIEC), es uno de los pocos organismos gubernamentales que aprovecha la tecnología biométrica para agilizar el proceso de identificación de personas, reduciendo tiempos y permitiendo a los usuarios acceder a los beneficios que dicho proceso logra obtener a partir de la biometría. De acuerdo con Registro Nacional de Identificación y Estado Civil (2010), El objetivo del servicio, es mejorar el tiempo de proceso de identificación de las personas, asimismo, permitir un procesamiento de la información ágil y seguro.

Las políticas de la seguridad informática son un conjunto de lineamientos que establecen el marco de referencia sobre las que sustentan las normas y/o procedimientos, los cuales son el canal formal de actuación del personal en relación

con los recursos y servicios informáticos. (Instituto del Mar del Perú, 2012).

Las políticas de seguridad son de gran importancia y totalmente útiles para mantener una estructura de seguridad estable, pero no constituyen una garantía para la misma si se conceptualizan por sí solas, ello depende del grado de esfuerzo del personal o colaboradores de la organización por asegurar que se cumplan dichas políticas de seguridad.

Se observó que la Empresa de Servicio de Agua Potable y Alcantarillado de Lima-SEDAPAL, mantiene una disciplinada y colaborativa labor frente a la sociedad, así mismo hacia el enfoque interno de su organización. Además, se constató que la información que SEDAPAL considera como activo importante, se asegura bajo estrictas medidas de seguridad de la información. Es por ello que, en un progresivo avance tecnológico donde los sistemas de información se han incorporado en la gestión estratégica, generando grandes volúmenes de datos, que se considera totalmente importante y valiosa en la toma de decisiones, SEDAPAL trabaja constantemente en mantener la información confidencial, disponible y totalmente íntegra para su uso objetivo, asimismo, la estructura de seguridad que mantiene SEDAPAL es eficaz para sus fines, debido a que desarrolla un marco de trabajo estable, como son los recursos que gestionan la información, los mecanismos y técnicas de control de seguridad internos, el uso de programas especializados, como también el acceso estructurado de los usuarios.

En este sentido es que se restringe el acceso no autorizado a la información mediante el control de usuarios y contraseñas, la cual se concibe en una metodología eficaz; sin embargo, como cualquier sistema orientado al uso de este mecanismo, es susceptible a diversas vulnerabilidades, tales como suplantación de identidad, robo de claves de acceso, perdida u olvido de credenciales e incluso ataques de ingeniería social; representando una amenaza inminente a la información, elevando su grado de exposición y asumiendo los riesgos asociados, tales como eliminación, pérdida, modificación, o robo de información; estas acciones provocarían un conflicto en cuanto a la validez y autenticidad de la información como también puntos de quiebre en su estructura de seguridad. Ante esta problemática se establece que la biometría es una

herramienta efectiva para el control de acceso a la información, pues es necesario el reconocimiento físico inequívoco de la persona autorizada a utilizar la información, ello permite la autenticación o proceso de que alguien es quien dice ser.

1.2. Formulación del problema

1.2.1. General

¿De qué manera influye la aplicación de reconocimiento biométrico por huella dactilar en la seguridad lógica en SEDAPAL, 2020?

1.2.2. Específicos

a) ¿De qué manera influye la aplicación de reconocimiento biométrico por huella dactilar en el control de acceso en SEDAPAL, 2020?

b) ¿De qué manera influye la aplicación de reconocimiento biométrico por huella dactilar en la Ingeniería Social en SEDAPAL, 2020?

c) ¿De qué manera influye la aplicación de reconocimiento biométrico por huella dactilar en las Auditoria de seguridad en SEDAPAL, 2020?

1.3. Justificación

La presente investigación se enfoca en demostrar la influencia de una aplicación de reconocimiento biométrico por huella dactilar en la seguridad lógica en SEDAPAL - Servicio de Agua Potable y Alcantarillado de Lima, debido a que en la actualidad la seguridad de la información resulta ser un factor de suma importancia para toda organización, especialmente por el constante crecimiento tecnológico y los riesgos asociados que este conlleva.

1.3.1. Institucional

A nivel institucional, SEDAPAL es reconocida por ser una entidad estatal peruana, líder en la prestación de servicios de agua potable, alcantarillado y tratamiento de aguas residuales, bajo los más altos estándares de calidad, consignando el desarrollo de sus actividades de forma eficiente y responsable desplegado a todos sus niveles en servicio de la población que atiende. Es por ello que, el fortalecimiento de la seguridad

y gestión de la información, forma parte de uno de los procesos más importantes y con un tratamiento especial en la organización orientado a la mejora continua. Es por todo lo mencionado, que la aplicación de la presente investigación pretende demostrar la mejora de los aspectos relacionados a la seguridad, quien en su constitución converge al principal activo en combinación con su desarrollo institucional. En definitiva, la información se manifiesta a partir de diversos medios de gestión, los cuales garantizan su integridad, disponibilidad y confidencialidad a partir de los mecanismos de acceso que se proporcione para protegerla, sin embargo, se explicará las diversas modalidades que puedan comprometer su veracidad y autenticidad, los cuales resultarían en la afectación diversificada a la imagen corporativa.

1.3.2. Operativo

A nivel operativo, la implementación de la presente investigación se orienta a tres objetivos principales en mención, los cuales se enfocan directamente en el proceso operativo, productivo y funcional por parte del personal asignado en relación a la interacción con los sistemas de información. La seguridad como objetivo principal en función a la autenticación de los usuarios y el control de acceso sobre los sistemas de información, la confiabilidad como segundo objetivo en función a la eficiencia y funcionamiento de la aplicación, y finalmente la gestión como tercer objetivo en función a la eficacia y usabilidad de la aplicación. La coordinación e integración de todos los elementos indicados implican un incremento en la productividad como consecuencia de un proceso operativo, el cual contempla diferentes aspectos que suponen mejoras en concordancia a los objetivos empresariales por la organización.

1.3.3. Tecnológico

A través de las tecnologías de la información y Comunicaciones, las organizaciones van cambiando su modo de operación en la forma en la que se comunican y desarrollan. El crecimiento tecnológico y la inserción de las nuevas TIC’s en la gestión de las organizaciones requiere un tratamiento especial y mayor atención por parte de la alta dirección, responsable del despliegue de las directivas a todos los miembros de la empresa, orientado al logro de los objetivos, por lo que es necesario contar con un

plan estratégico de tecnologías de información y comunicaciones (PETIC) destinado al modo de uso y optimización de los recursos informáticos. Este documento es la herramienta que permita ordenar los esfuerzos de incorporación de las TIC en la organización y sus procesos. Establece los lineamientos requeridos para controlar la adquisición, uso y la administración de los recursos de TIC. La presente investigación considera cada punto establecido en el PETIC como guía para la implementación del mismo, por ende, se pretende reforzar la seguridad aplicando un modelo de reconocimiento por huella dactilar para los sistemas de información almacenada en las aplicaciones (seguridad lógica), realizándose dentro de un equipo funcional, siendo piloto para una posterior implementación a todo nivel.

1.3.4. Económico

A nivel económico, SEDAPAL mantiene el compromiso permanente en asegurar la sostenibilidad financiera de la empresa, lo que implica una serie de actividades que se desarrollan de forma constante a fin de evaluar las mejores condiciones para el correcto desempeño de la organización en cada uno de sus procesos y respectivas áreas de ejecución, a través de la provisión de los recursos necesarios e indispensables para la continuidad de las actividades. En este aspecto el campo tecnológico resulta ser un gran aliado para SEDAPAL, siendo uno de los principales agentes generadores de recursos para la organización en el logro de sus objetivos empresariales.

1.4. Objetivos

1.4.1. General

Determinar de qué manera influye la aplicación de reconocimiento biométrico por huella dactilar en la seguridad lógica en SEDAPAL, 2020.

1.4.2. Específicos

a) Explicar de qué manera influye la aplicación de reconocimiento biométrico por huella dactilar en el control de acceso en SEDAPAL, 2020.

b) Describir de qué manera influye la aplicación de reconocimiento biométrico por huella dactilar en la ingeniería social en SEDAPAL, 2020.

c) Mencionar de qué manera influye la aplicación de reconocimiento biométrico por huella dactilar en la auditoria de seguridad en SEDAPAL, 2020.

1.5. Hipótesis

1.5.1. General

La aplicación de reconocimiento biométrico por huella dactilar si influye en la seguridad lógica en SEDAPAL, 2020.

1.5.2. Específicos

a) La aplicación de reconocimiento biométrico por huella dactilar si influye en el control de acceso en SEDAPAL, 2020.

b) La aplicación de reconocimiento biométrico por huella dactilar si influye en la Ingeniería Social en SEDAPAL, 2020.

c) c) La aplicación de reconocimiento biométrico por huella dactilar si influye en las auditoria de seguridad en SEDAPAL, 2020.

II. MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes Nacionales

Monjaraz (2015) realizó una Investigación en Perú, en la Universidad Científica del Sur, titulada: “Estudio de pre factibilidad para implementar biometría mediante huella digital en la red de cajeros automáticos, Banco de Crédito del Perú”, con el objetivo de desarrollar un estudio de pre factibilidad para presentar una nueva forma de acceso a los servicios de cajeros automáticos implementando lectura biométrica por huella dactilar, y sus usos. Esta Tesis conforma la siguiente metodología, investigación aplicada de tipo descriptiva y explicativa, con un diseño no experimental con enfoque cualitativo. Alcanzó el resultado de intervalos de confianza sólidos, tras haber cumplido con los criterios que jueces expertos consideran obligatorios y al examinar las grandes oportunidades que la aplicación tendría en el negocio y en el país. Además de obtener una reducción de las vulnerabilidades se seguridad que el proceso de identificación actual trae consigo, menores perdidas al negocio por fraude bancario y a nivel de competitividad se posicionó a la entidad financiera en el primer lugar respecto a las funcionalidades en el canal de cajeros automáticos. Concluye que los sistemas biométricos son la mejor alternativa en el país para lograr una correcta y rápida autenticación, aumentando considerablemente la seguridad, asimismo, que la innovación tecnológica debe ir acompañada de procesos internos que la soporten, y que el personal esté debidamente capacitado para poder llevarlo adelante. Aporta la recomendación a corto plazo de que el proveedor Diebold inicie pruebas en laboratorio con el lector biométrico Lumidimg en los cajeros automáticos del Banco, que se brinde funcionalidad de pago de servicios con empresas más representativas, configurar el sistemas de los cajeros para soportar una nueva funcionalidad de entrega de duplicado de tarjeta de débito; por otro lado la recomendación a largo plazo es de que el banco deberá prepararse para apoyar el proceso de difusión y adopción del DNI, desplegar la lectura biométrica de huellas dactilares en el resto de cajeros automáticos del canal y luego hacer el estudio para otros canales, adaptar los procesos y arquitectura del Banco para tener una visión 360° del cliente y lograr una lógica de prospección para

identificar ‘no clientes’ con potencial en base a sus transacciones reveladas y así aprovecharla comercialmente.

Marín (2017) realizó una investigación en Perú, en la Universidad Tecnológica del Perú, titulada: “Propuesta de mejora de un sistema biométrico multiusuario para cajeros automáticos en instituciones bancarias en la ciudad de lima - 2017”, con el objetivo de desarrollar un buen sistema biométrico facial multiusuario para mejorar la seguridad de los cajeros automáticos que minimicen los riesgos de las personas al efectuar transacciones. Llego a la conclusión que la realización del sistema influye principalmente para tener los mejores resultados, ya que sin un buen bosquejo de seguridad con todas las bases de datos de los clientes principales y/o secundarios, no se puede obtener un buen nivel de reconocimiento facial, también indicó que los sistemas biométricos no son perfectos al 100%, sin embargo, considera que estos actualmente son la mejor alternativa en el país para lograr una correcta y rápida autenticación, aumentando considerablemente la seguridad.

Llatas (2015) realizó una Investigación en Perú, en la Pontifica Universidad Católica del Perú, titulada: “El registro biométrico dactilar con el sistema AFIS y el control del delito”, con el objetivo de analizar la implementación del sistema AFIS y determinar el impacto que tienen en la identificación certera de personas involucradas en un acto delictivo. Concluye que se requiere de personal que este correctamente capacitado para su manejo. En este sentido, el hecho de que estas labores este conformado por peritos antiguos acostumbrados a otro sistema de trabajo, hace que tanto la capacitación como la adaptación a este sistema sea más difícil. Además, se observó que el sistema AFIS policial enfrenta problemas de raíz, como la capacitación correcta de los peritos, pero también en la gestión de espacios adecuados; estos hechos parecen afectar la motivación del personal y podría afectar la efectividad de sus dictámenes periciales. Aportó la recomendación de implementar una infraestructura más adecuada para el mejor desempeño y desarrollo profesional de las actividades o funciones que realizan los expertos en el manejo del sistema AFIS policial, además de contar con personal debidamente capacitado en el manejo del software y por ultimo de manera de retroalimentación se requiere que exista una norma legal que sustente los

procedimientos del AFIS policial, que determine técnica y científicamente su producto como un elemento de prueba que contribuya a la investigación policial teniendo como objetivo la identificación plena de los autores de hechos criminales.

Inoguchi y Macha (2015) realizaron una Investigación en Perú, en la Universidad San Ignacio de Loyola, titulada: “Gestión de la ciberseguridad de los ataques cibernéticos en las PYMES del Perú”, con el objetivo de determinar la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, 2016. Esta Tesis sigue la siguiente metodología, investigación cuantitativa de nivel descriptivo, con un diseño no experimental. Alcanzo el resultado de que para el personal consultado de la Empresa Transporte Zavala Cargo S.A.C, la seguridad es muy importante; sin embargo, la empresa no cuenta con procedimientos ni políticas que orienten a las buenas prácticas en el uso de la tecnología, no ha formado a sus empleados en materia de ciberseguridad para prevenir y evitar posibles amenazas; no invierten en herramientas de seguridad y no tienen personal responsable de la seguridad de la empresa en la red. Concluye que La Empresa Zavala Cargo S.A.C. tiene una falta del uso de planes contra ataques de Seguridad Cibernética, que resguarden su información cibernética permitiendo así una toma de decisiones más confiable, además agregó la falta de apoyo económico al proceso de creación de medidas de seguridad informática dentro de una red privada, provocando así que la organización se exponga a mayores riesgos. Recomendó elaborar políticas de ciberseguridad en la empresa, con la finalidad de que su personal comprenda la importancia de esta materia, además de ejecutar auditorías a la ciberseguridad de su empresa con la finalidad de conocer las flaquezas de seguridad informática y que procedimientos se debe realizar para menguar los riesgos.

Araujo y Linares (2018) realizó una investigación en Perú, en la Universidad Peruana de Ciencias Aplicadas, titulada: “Desarrollo de aplicaciones biométricas y cognitivas para un modelo de espejo inteligente”, con el objetivo de desarrollar aplicaciones cognitivas en un modelo de espejo inteligente con autenticación de reconocimiento facial cuya interacción a los servicios de información como fecha, hora, clima, agenda, correo se realice mediante el reconocimiento de voz y la integración de un algoritmo

de clasificación de Naive Bayes para la personalización de noticias. Llego a la conclusión de que los espejos inteligentes tienen un gran potencial para ayudar a los usuarios a acceder e interactuar con la información necesaria sin esfuerzo. Como resultado de las investigaciones sobre dispositivos con la superficie de un espejo, se ha diseñado un espejo inteligente que permite al usuario acceder e interactuar con la información, mejorando la experiencia de este mediante la personalización por medio de un sistema de recomendación de noticias. Además, con el fin de mejorar la experiencia de usuario que brinda nuestro espejo también se implementó la funcionalidad de reconocimiento de comandos de voz para mejorar la interacción del espejo y esta lea la información que presenta en su interfaz. Aportó la recomendación de obtener más instancias en el dataset para mejorar la precisión de la predicción de las noticias, también de contar con un repositorio para retrasar o depender de los avances de otra persona, además de contar con un backup y guía de despliegue del proyecto por seguridad en caso de que se tenga problemas técnicos en el servidor actual.

2.1.2. Antecedentes Internacionales

Hernández (2016) realizó una investigación en México, en la Universidad Autónoma del Estado de México, titulada: “Autenticación biométrica a través de huellas digitales e iris en una empresa industrial”, se planteó como objetivo de investigación realizar una identificación de personas por medio del reconocimiento digital de imágenes biométricas. Concluyó que, la necesidad de tener un sistema de seguridad ya sea para control de acceso o autenticación de individuo ha llevado estar buscando nuevas alternativas de sistemas. Los sistemas biométricos empleados para el control de seguridad cada día son más seguros, ya que maneja grandes ventajas de identificar quien es no que trae, como es las características únicas de cada individuo que lo hace ser único. Estos sistemas no recurren al uso de claves personalizadas, tarjetas, llaves, entre otras los cuales son fácilmente de robar o clonar. Sino al proceso de autenticar biométricamente con iris y huella dactilar, esto da una mayor confiabilidad en la seguridad puesto si solo la huella dactilar es un sistema con mayor confiabilidad ahora creando un sistema con dos biométrico, esto duplicará el porcentaje de seguridad, ya

que anteriormente para la huella dactilar existían mecanismos para clonar o duplicar una huella dactilar, (aunque estos mecanismos son costoso), en el caso que llegará a pasar el sistema puede reconocer a la persona por la huella dactilar, pero el sistema también requiere el iris de la persona o no podrá tener acceso. El objetivo principal de esta investigación se cumplió, a través de la propuesta del sistema de autenticación biométrica a través de huella dactilar e iris de los cuales los elementos principales son el lector de huella dactilar y el lector de iris, así como también la base de datos que va a guardar toda la información de los empleados. El sistema puede ser ocupado no solo en el ámbito industrial también en sector público y privado como puede ser una escuela privada para el acceso de sus alumnos como también hospitales de control de sus doctores. El así también el objetivo como estudiante de ingeniería en computación se concreta en otros más específicos relacionados con la formación teórica y la practica adquirida al realizar la propuesta de sistema de autenticación biométrica.

Montaña (2017) realizó una investigación en Colombia, en la Universidad Libre Sede Bosque Popular, titulada: “Sistema de identificación mediante huella digital para el control de accesos a la Universidad Libre Sede Bosque Popular simulado en un entorno web”, con el objetivo de desarrollar un sistema de identificación por huella digital para control de accesos de la Universidad Libre Sede Bosque Popular simulado en un entorno web. Esta Tesis se centra en el análisis respectivo en la manera de cómo se deben utilizar los recursos tecnológicos para lograr el cumplimiento de los objetivos de este proyecto. Alcanzo los resultados en base a treinta encuestas realizadas, evidenciando que la mayoría de encuestados (56%) son mujeres y (44%) hombres, en cuanto a que, si piensa que los sistemas de control de accesos de personal son esenciales e importantes, el 100% de los encuestados dijeron que sí. Concluyendo que la comunidad estudiantil de la Universidad libre sin importar el género, desean sentirse seguros con sus objetos personales, dentro de las instalaciones de la sede bosque popular de la universidad libre. Se hace necesario que la institución implemente un sistema de control de accesos que sirva como colaboración a la celaduría, con el fin de tener control de las personas que ingresan y que salen de la sede.

Escajedo (2015) realizó una investigación en España, en la Universidad de Alicante, titulada: “Reconocimiento e identificación de las personas mediante biometrías estáticas y dinámicas”, con el objetivo es abordar la realidad de los sistemas biométricos contemporáneos, concluyendo que el reconocimiento biométrico tradicional y el contemporáneo coinciden en su afán por captar métricamente la singularidad de cada persona respecto de un rasgo biológico (estático o dinámico) que es considerado universal y permanente en los seres humanos, además agregó que lo que las distingue es que en la contemporánea, los sistemas de reconocimiento son automatizados. Ese componente de automatización se considera tal esencial que es el argumento por el cual buena parte de la literatura excluye al ADN del elenco de características que pueden servir de base a un sistema de reconocimiento biométrico en el sentido moderno de la expresión, toda vez que no existe aún una tecnología capaz de realizar de forma automatizada el proceso de captación, análisis y comparación de patrones ADN.

Vallejo y Carrera (2017) realizó una investigación en Ecuador, en la Escuela Superior Politécnica de Chimborazo, titulada: “Implementación de un sistema biométrico de huellas dactilares para el control de asistencia estudiantil en la escuela de Ingeniería Industrial de la Facultad de Mecánica”, con el objetivo de implementar un sistema biométrico de huellas dactilares para el control de asistencia estudiantil en la Escuela de Ingeniería Industrial de la Facultad de Mecánica. Obtuvo el resultado empleando con la técnica de la encuesta con un banco de preguntas a los estudiantes de los 6 cursos con una muestra de 178 estudiantes, el resultado de los datos muestra que hay una gran aceptación del sistema implementado en todas las preguntas se obtuvieron un porcentaje mayor al 90%. Concluye que al implementar los equipos biométricos y el software attendance management se automatizó el proceso de control de asistencia tradicional, además que se seleccionó el software Attendance Management por sus amplias características que permitieron cumplir con la programación deseada, obteniendo reportes de asistencia de una manera rápida, segura y eficiente. Por otro lado, se determinó que el método actual automatizado tiene mayor aceptación que el método tradicional, ya que los datos obtenidos del mismo son rápidos, confiables y es

un gran aporte al avance tecnológico de la Escuela de Ingeniería Industrial. Aportó la recomendación de realizar una ligera presión del dedo para que el área escaneada sea mayor para así lograr identificar y registrar al estudiante.

Sánchez (2015) realizó una investigación en España, en la Universidad Carlos III de Madrid, titulada: “Estudio del rendimiento biométrico de sistemas de huella dactilar. Análisis de diferentes sensores y algoritmos”, con el objetivo de realizar un análisis a través de una evaluación de rendimiento tecnológico, en el que se pretende obtener un resultado aclaratorio de la comparativa entre dos algoritmos utilizados en la modalidad de huella dactilar tras la obtención de una base de datos mediante tres sensores diferentes. Obtuvo el resultado indicando que el estudio está realizado bajo una base de datos reducida, por lo que el número de muestras utilizadas es menor. Lo ideal hubiera sido utilizar la base de datos al completo, dado que la biometría se basa en probabilidad, pero el coste computacional hubiese sido demasiado elevado. Concluye que se ha implementado correctamente una aplicación capaz de realizar las comparaciones de varias muestras obtenidas con tres sensores distintos y bajo el uso de dos algoritmos diferentes. Además de haber implementado otra aplicación encargada de analizar los resultados obtenidos y aportar las medidas de rendimiento. Asimismo, que con el desarrollo de ambas aplicaciones se consigue cumplir con los objetivos marcados para este proyecto en el que se debía realizar una evaluación de rendimiento tecnológica sobre dos algoritmos, efectuando un posterior análisis de los resultados obtenidos.

2.2. Bases Teóricas

2.2.1. Bases teóricas de la variable independiente

Definición formal de la biometría

La biometría se conceptualiza como una tecnología de reconocimiento de patrones únicos e intransferibles, los cuales tienen un enfoque de seguridad a través de mecanismos como el control de acceso. Das (2015) describe a la biometría como el uso de la tecnología de la informática para extraer las particularidades únicas de un

individuo, de acuerdo a aspectos físicos o de comportamiento, con el fin de verificar la identidad del mismo (p. 6).

De acuerdo a lo anterior, la biometría ocupa un rol fundamental en la seguridad de una organización sin importar su estructura, esta tecnología está orientada a respaldar los activos que la organización posee, teniendo como principal objetivo autentificar a un individuo por medio de una correcta gestión de credenciales suministradas por la organización, las cuales permitirán o denegarán el acceso a los recursos y su posterior uso.

La necesidad de la biometría

En referencia a la biometría como una tecnología de reconocimiento efectiva en base a los patrones propios de un individuo, esta puede tomar diversas formas de medición para llevar a cabo su objetivo.

Según Marcel, Nixon, y Li (2014) afirman que “la necesidad y la complejidad del reconocimiento de los seres humanos nunca han sido tan grande en nuestra historia como lo es ahora y la biometría es considerada como una herramienta indispensable para superar las dificultades que se enfrentan” (p. 1).

Lo esencial para una organización es que sus recursos constituyan seguridad en todo su concepto, para ello la biometría se presenta como el punto central para que este enfoque se cumpla. Las intenciones de un individuo, sea externo o interno a la organización, pueden atentar contra los activos y desatar diversos problemas que pongan en riesgo a la organización y sus fines; la biometría es muy importante porque desempeña un rol imprescindible en la protección de los activos.

Estructura general de un sistema biométrico

Un sistema es un conjunto de elementos que sostienen una interrelación orientada a un fin en común, llevándolo hacia el concepto de tecnologías biométricas, es la combinación del reconocimiento de patrones a través de un conjunto de elementos de captura, procesamiento y acopio que tienen como fin la medición de una característica única del individuo.

Según Ortega, Fernández y Coomonte (2008) manifiestan que un sistema biométrico es un reconocedor de patrones que obtiene las características y las compara con otros patrones almacenados en el sistema. Este sistema se compone por siete fases, empezando con la adquisición de datos, en la cual se recogen los datos. Es determinante, debido a que la cantidad y la calidad de la información adquirida resulta ser importante para las fases siguientes. Por otro lado, en el pre procesado de la información es necesario la corrección de cualquier distorsión captada en la recopilación de datos. Por otra parte, se elimina la información que no resulte necesaria para el procesamiento. De este modo, se extraen únicamente aquellas características que sean pertinentes. Posteriormente se elabora un modelo que personifica a cada individuo, estos modelos se almacenan en una base de datos, iniciando la comparación entre los datos brindados con los que se encuentran almacenados, para que de esa manera se determine si los datos del individuo coinciden con de la base de datos. (pp. 15 - 16).

En el proceso del sistema biométrico, se pueden destacar algunos puntos significativos de acuerdo a cada parte del mismo; la calidad de captura es un punto determinante debido a que este elemento es brindado por el individuo, por ello, la calidad podría ser afectada por diversos factores que la pueden degradar; por ejemplo, la suciedad, el movimiento excesivo del dedo, humedad, entre otros. En lo que refiere al pre procesado, se considera como un normalizador para que los factores mencionados que degradan la imagen capturada sean corregidos para su posterior procesamiento. Por último, el umbral de decisión infiere en que los datos capturados hayan sido recogidos correctamente, en este contexto, no solo depende de que el rasgo biométrico del individuo se encuentre almacenado en el sistema o no, sino de que el umbral de decisión realice su proceso de acuerdo a unos datos biométricos de calidad.

Reconocimiento biométrico

La biometría es una tecnología de autenticación basada en el reconocimiento inequívoco de las propiedades únicas e intransferibles de un individuo.

De acuerdo con Serratosa (2012) explica que el reconocimiento biométrico se refiere al uso de diversas características anatómicas, los cuales se denominan identificadores biométricos que sirven para garantizar la identidad de un individuo (p. 14)

Según Jain, Flynn & Ross (2008), el reconocimiento biométrico es la ciencia de establecer la identidad de un individuo en función de los atributos físicos o de comportamiento de la persona. (p. 2)

De acuerdo con Boulgouris, Plataniotis & Tzanakou (2010), la base del reconocimiento biométrico para identificación de un individuo en particular se rige por rasgos fiscos característicos o de conducta propios de cada uno. En la actualidad los sistemas biométricos forman parte fundamental en la seguridad de grandes arquitecturas.

El reconocimiento biométrico en combinación con componentes sistematizados que proporciona una estructura de seguridad fortificada conducente a la autenticación univoca de individuos, debido a que esta no depende de factores que puedan ser extraviados o hurtados, sino que funciona como un mecanismo individual e intransferible propio de cada persona.

Segmentos típicos del mercado biométrico

Actualmente esta tecnología está tomando un mayor protagonismo en el mercado orientado a la protección de datos, a través del control de acceso con el uso de mecanismos que permitan identificar a un individuo y brindarle la autorización correspondiente.

Según Das (2015) sostiene que las tecnologías biométricas pueden servir a casi cualquier industria o mercado donde sea necesario implementar un modelo de seguridad o mejorar el nivel de una infraestructura de seguridad existente. Además, señala que la biometría viene remplazando varias formas de acceso por medio de contraseñas, denominándolo como una herramienta de único acceso (pp. 40 - 41).

Generalmente las organizaciones utilicen aun los mecanismos tradicionales de control de acceso, como las tarjetas de acceso o contraseñas, sin tener en consideración aspectos que degradan su credibilidad y confiabilidad; por ejemplo el robo de credenciales de acceso, sabotaje entre empleados, la pérdida u olvido de contraseñas,

que equivocadamente algunas políticas exigen volverlas más complejas, para que de este modo sea casi indescifrable, sin embargo lo que no prevén es que al exigir este método de seguridad, aumentan la posibilidad a que el usuario gestione ineficientemente sus credenciales.

Ventajas del reconocimiento biométrico sobre las técnicas tradicionales de autenticación

Los procesos de autenticación tradicionales como tarjetas de acceso o contraseñas se han utilizado por mucho tiempo, pretendiendo resguardar la seguridad de los recursos por medio del control de acceso.

Ortega, Fernández y Coomonte (2008) aseveran que la autenticación personal no es un problema reciente, sino que la sociedad hace décadas que ha adoptado ampliamente mecanismos para reconocer individuos. Por otro lado, las personas suelen compartir sus credenciales con otros individuos, esto deriva a que no se pueda determinar con certeza quien es la persona que ingresa al sistema (pp. 9 - 11).

De acuerdo a lo anterior, los métodos tradicionales han sido eficaces, pero han representado una serie de inconvenientes, los cuales ponen en riesgo la información, asimismo, los conceptos que los representan, tales como la disponibilidad, integridad y confidencialidad. Por ello, que el reconocimiento por huella dactilar promueve en un sentido sustancial a la protección de estos recursos que están directa e indirectamente vulnerables a la mayor amenaza para la información, el fallo humano.

Los componentes granulares del reconocimiento

Es importante tener en claro que no todo sistema de reconocimiento trabaja de la misma manera, hay algunos que priorizan un mayor análisis a su extracción de características, pero ajustando el concepto, el principio de un sistema podría basarse si es por verificación o identificación.

Según Das (2015) afirma que es cierto que el sistema biométrico está tratando de determinar quién es usted en un nivel general. Sin embargo, hay mucho más que sucede en el nivel granular de reconocimiento. Por lo tanto, es necesario dividir los

componentes individuales del reconocimiento en la verificación, identificación, autenticación y la autorización (pp. 9).

Como se mencionó anteriormente, la verificación y la identificación pueden ser el punto de partida del reconocimiento con la única diferencia de que la verificación se orienta a comparar el dato biométrico ingresado con otro inscrito previamente, mientras que la identificación tiene el enfoque de comparar el dato biométrico ingresado con otros datos biométricos de una base datos. Posteriormente a esto, la autenticación es la aprobación o aceptación de que el resultado de la comparación ha sido exitosa y admitida por el sistema de procesamiento biométrico. La autorización resulta ser el permiso para disponer de los recursos que estamos acreditados a usar.

Huella dactilar

En la actualidad, la huella dactilar es el rasgo biométrico más utilizado para la autenticación de personas, debido a su sencillo modelo de desarrollo y bajo coste de implementación.

De acuerdo con Ortega, Fernández y Coomonte (2008) la composición de la huella dactilar se basa en un patrón de crestas y valles, los cuales se encuentran ubicados en la parte superior del dedo, habiéndose formado a partir de los primeros meses en que el feto se desarrolla y permaneciendo hasta el final del proceso de descomposición por defunción.

Durante mucho tiempo previo a los sistemas automatizados, la captura de huellas dactilares se realizaba utilizando tinta y papel para su almacenamiento. Hoy en dia gracias al permanente crecimiento tecnológico, se cuenta con hardware y software avanzado que en combinación permiten que este proceso sea realizado de forma automatizada.

Características Físicas

Cada persona posee características únicas e intransferibles, asimismo sucede con cada rasgo individualizado correspondiente a las huellas dactilares, ni siquiera dos personas tienen las mismas huellas, lo que hace a este tipo de identificación una herramienta valiosa.

Komarinski (2005) afirma que las crestas en los dedos se crean durante el desarrollo del embrión en respuesta a las presiones que forman patrones que pueden ser clasificados por los examinadores de impresión. Proporcionan una superficie relativamente rugosa, lo que hace posible agarrar y sujetar los objetos con facilidad. Cada cresta contiene al menos un poro, que está conectado a una glándula sudorípara debajo de la piel.

La glándula sudorípara ayuda a eliminar los residuos del área de la cresta, así como a mantener una temperatura relativamente constante a través de la evaporación. El sudor producido es también la fuente de depósitos para las impresiones latentes, es decir, aquellas imágenes de los dedos que permanecen sobre una superficie después de haber sido tocadas. (pp. 61-62)

Una huella dactilar es la impresión moldeada que produce el contacto de un dedo de la mano sobre una superficie. Además, la huella dactilar representa una característica perenne, porque permanecen indefectiblemente invariables en el tiempo, como también son inmutables, ya que las huellas dactilares no pueden modificarse fisiológicamente, son diversiformes, pues no se ha hallado todavía dos impresiones idénticas derivadas por dedos diferentes, y son originales, ya que todo empalme directo produce impresiones originales con características microscópicas identificables del tejido epidérmico. Por lo tanto, la huella dactilar representa en esencia la identidad de una persona de una forma única e intransferible.

Reconocimiento de huellas dactilares

El reconocimiento de huellas dactilares es conocido como uno de los métodos más usados, con un alto nivel de aceptación, enfocado a la identificación de individuos, basándose en las características físicas del mismo.

Según Das (2015) considera elementos que caracterizan las ventajas de esta tecnología, consolidando conceptos como universalidad, unicidad, permanencia, colectabilidad, rendimiento y aceptabilidad (pp. 59 - 62).

Examinando cada punto, la universalidad conceptualiza a que todo el mundo tiene este rasgo, sin embargo, hay excepciones en las que no se posee, tales son amputaciones, quemaduras, malformaciones, entre otros aspectos.

La unicidad refiere a que no hay dos individuos con las huellas dactilares idénticas, sin embargo, no existe un estudio científico fiable que pueda comprobar esta teoría, puesto que se tendría que comparar todas las huellas dactilares del mundo para determinar su completa fiabilidad.

La permanencia define que las características no cambian a través del tiempo, es decir si un individuo envejece su rasgo persistirá, pero obviamente esta premisa puede encontrarse involucrada en problemas con un entorno deficiente en el que sea imposible capturar un dato de calidad.

Respecto al rendimiento, se ramifica hacia diversos aspectos del procedimiento como es la fase de captura, extracción de datos, comparación, entre otros, es decir, este elemento depende mucho de los algoritmos que se utilicen para el procesamiento de huellas dactilares. Das (2015) explica que es necesario un sensor para obtener la imagen de la cual se extraerán y analizarán las características capturadas. Posteriormente se aplica ciertos algoritmos que son necesarios para filtrar las características del individuo (pp. 5 - 6).

La aceptabilidad puede resultar afectada dependiendo de la concordancia de los puntos anteriores, aunque la mayoría de opiniones respecto al reconocimiento de huellas dactilares resultan ser muy favorables.

AFIS – Sistema de identificación automatizada de huella dactilar

El AFIS es un sistema informático compuesto de hardware y software integrados, que permite obtener, procesar y verificar de forma automatizada las huellas dactilares.

Komarinski (2005) explica que el desarrollo de los AFIS fue realizado como respuesta a la importancia que resultaba poder contar con sistemas identificación agiles y su vez precisos.

En esencia AFIS representa una forma más solidificada que la identificación tradicional interpuesta por varios años, esto es por la combinación de componentes altamente calificados de hardware orientados a la captura y procesamiento del rasgo biométrico de huella dactilar y el software que se complementa como una parte fundamental. Además de integrarse en la visión de constante desarrollo, para que conceptos como precisión, velocidad, escalabilidad, estabilidad, seguridad, entre otros, vuelvan más efectivo este sistema.

Seguridad del sistema biométrico

Se puede argumentar respecto a la seguridad, que los métodos tradicionales en comparación con la biometría, representan una deficiencia en cuanto a confidencialidad, integridad y disponibilidad de la información, desventajas aprovechadas por individuos, que tienen el afán de corromper el sistema.

Marcel, Nixon y Li (2014) mencionan que, los rasgos biométricos siendo elementos únicos y fuertemente relacionados a un usuario en específico, pueden ser argumentados como seguros, ya que posea cierta ventaja sobre los demás, la cual permite verificar la identidad de un individuo de forma más confiable a comparación de los métodos tradicionales como contraseñas, que podrían ser comprometidas con un menor nivel de dificultad para diversos fines.

La falta de conocimiento en cuanto a temas de huellas dactilares, permite a que los intrusos tengan la libertad de apoderarse de ellas, debido a que las huellas dactilares por cuestiones de composición en combinación con el entorno, es decir, la segregación de sustancias naturales que el cuerpo emana tales como el sudor o la grasa corporal en combinación con algún componente externo, es un medio por el cual es seguro dejar la huella dactilar en casi cualquier superficie. Por lo tanto, esto beneficia al agente de amenaza para obtener esa muestra y poder falsificar modelos que permitan utilizarse para fines ilícitos. La desventaja de ello es que el individuo poseedor de la huella dactilar original no estará pendiente de las huellas dactilares que deja en cada lugar en el que la huella tiene contacto, lo que hace que sea un elemento de fácil posesión.

Biometría Anti-Falsificación

En el reconocimiento biométrico, existen especialistas que se encargan de detectar las tentativas para vulnerar dispositivos biométricos, principalmente cuando el usuario presenta su huella biométrica al sistema. Con este enfoque, los investigadores analizan qué trampas se pueden presentar, para así mejorar los sistemas biométricos ya existentes.

Según Marcel, Nixon y Li (2014) mencionan que los especialistas de diferentes campos vienen trabajando en métodos que puedan combatir ataques y amenazas, en especial la suplantación de identidad. Este trabajo se basa en poder diferenciar la veracidad de una huella biométrica valida por una persona entre una falsa por un atacante.

Anti-falsificación consiste en descubrir todas las posibles tentativas fraudulentas para superar a un sistema biométrico, con el objetivo de que el sistema pueda identificar dicho intento de manera autónoma. Los expertos evalúan la efectividad de los sistemas biométricos, en correlación a varios tipos de ataques y crean algoritmos para detectar cualquier intento de fraude. Los retos en este aspecto son grandes, debido a que hay un constante duelo entre los avances tecnológicos en la seguridad y sus amenazas, porque cada vez están más competentes para atacar los modernos sistemas de seguridad. Por ello, los investigadores también trabajan en mecanismos que permitan que los sistemas biométricos sean más seguros

Estado de la técnica en la huella digital anti-falsificación

Diversas investigaciones han tratado de aportar y reforzar mecanismos de identificación de falsificaciones, respaldadas en las características propias de la huella dactilar.

Según Marcel, Nixon y Li (2014) sostienen que uno de los principales esfuerzos para prevenir que las huellas dactilares sean falsificadas, originó que se realice una ruta de investigación, la cual se basa en analizar el patrón que permite la transpiración de la piel, que a comparación de un dedo falso (artificial) sería muy complicado de imitar.

De acuerdo a lo anterior, existen estudios importantes que sustentan características que apoyan a la biometría anti falsificación, la transpiración es un elemento importante

y principal dentro del concepto de la huella dactilar, pues supone una realidad de la misma a través de la segregación de las glándulas sebáceas. Por otro lado, la textura infiere mucho en la intensidad como en la temperatura de la superficie. Estos elementos conjeturan una combinación que es muy difícil de admitir en comparación de una copia de una huella dactilar.

Detección de la vida de la muestra

La estructura de la huella determina ciertos indicadores que hacen verdadera a una muestra, la vida de la muestra quiere aludir a ciertos elementos medibles para la identificación de una huella real.

Según Solé (2013) sostiene que “En sistemas basados en huellas dactilares, medidas de fácil detección como pueden ser la temperatura, la oximetría, la conductividad de la piel y la detección de capilares bajo la epidermis o el pulso cardíaco pueden dar mucha información sobre la vida de la muestra” (p.18).

Normalmente los elementos antes mencionados pueden determinarse bajo valores estandarizados, pero pueden presentar variaciones de acuerdo a cada individuo. La oximetría se refiere a la saturación de oxígeno en la sangre, la conductividad de la piel se refiere a los cambios de temperatura, electricidad de los nervios y sudor a través de la piel, capilares son pequeños vasos sanguíneos en la que circula la sangre, estos son algunos de los elementos que ayudan a identificar y a desechar muestras falsificadas, lo cual es un aporte grande para detectar amenazas.

Información general sobre seguridad biométrica

Se relaciona directamente a la biometría como mecanismo de seguridad, para el control de accesos lógicos y físicos, para el resguardo de los recursos de una organización, pero pasamos por alto las vulnerabilidades que este puede sufrir.

Jain, Flynn y Ross (2008) argumentan que los sistemas biométricos se implementan en equipos servidores, son vulnerables a todos los ataques criptográficos, virus y otros que afectan a los sistemas informáticos modernos.

- La evasión es un ataque que accede a los recursos protegidos por una medida técnica para subvertir el sistema biométrico. Un ataque de este tipo puede subvertir los sistemas informáticos subyacentes (sobrescribir decisiones de asignación o sustituir plantillas de base de datos) o puede implicar la repetición de datos válidos.
- La adquisición secreta (contaminación) es el uso de información biométrica capturada de usuarios legítimos para acceder a un sistema.
- La colusión y la coerción son vulnerabilidades del sistema biométrico de los usuarios legítimos del sistema. La distinción es que, en la colusión, el usuario legítimo está dispuesto (quizás por soborno), mientras que el usuario coaccionado no es (a través de una amenaza física o chantaje). Tales vulnerabilidades pasan por alto el sistema de seguridad de la computadora, ya que las características biométricas son legítimas.
- La negación de servicio es un ataque que impide el uso legítimo del sistema biométrico. Esto puede tomar la forma de ralentizar o detener el sistema (a través de una sobrecarga de las solicitudes de red) o degradando el rendimiento.
- El repudio es el caso en el que el atacante niega el acceso al sistema. Un usuario corrupto puede negar sus acciones alegando que sus datos biométricos fueron "robados" (por adquisición encubierta o elusión) o que un usuario ilegítimo fue capaz de realizar las acciones debido a la falsa aceptación biométrica. (pp. 381 -383).

Como se mencionó anteriormente, la biometría es un mecanismo de seguridad orientado al control de acceso, y a pesar de brindar mayor seguridad en comparación con otros mecanismos, como cualquier sistema no es seguro en su totalidad, ya que puede poseer ciertas vulnerabilidades las cuales podrían ser aprovechadas por un atacante mediante métodos de intrusión que le permita acceder a los sistemas y realizar acciones tales como: extracción, clonación y/o modificación de datos biométricos. Otro aspecto a considerar por su peligrosidad y difícil detección es cuando un usuario autorizado facilita sus rasgos biometricos para que de este modo el ataque no sea manifestado, los motivos de esta facilitación pueden ser por sabotajes, sobornos, amenazas, entre otros.

2.2.2. Bases teóricas de la variable dependiente

Seguridad Lógica

Mantener la seguridad lógica en los recursos informáticos requiere de ciertos esfuerzos primarios, que radican en la confidencialidad, disponibilidad e integridad.

Escrivá et al. (2013) afirman que “La seguridad lógica es el conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas. Así como a garantizar el acceso a la información únicamente por personas autorizadas” (p. 45).

Según Hernández y Flórez (2011), seguridad lógica corresponde a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático. (pp. 222-233).

De acuerdo con Martos et. al. (2004), la seguridad lógica engloba el conjunto de operaciones y técnicas orientadas a la protección de la información contra la destrucción, la modificación, la divulgación indebida o el retraso en su gestión (p. 489)

Según Aldegani (1997), el objetivo de la seguridad lógica es mantener la Integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por computadora. (p. 22)

Las medidas aplicadas de forma integral están orientadas a reforzar la seguridad de la información manteniendo tanto la integridad como restricciones de acceso a la misma solo por quienes estén debidamente autorizados.

Principios de la seguridad informática

La mayoría de especialistas concuerdan en que ningún sistema es seguro en tu totalidad, es por ello, que debe haber esfuerzos por proteger la información elevando su seguridad a niveles aceptables para los usuarios y que cumplan con los siguientes 3 principios básicos:

Confidencialidad. Hace referencia ciertas restricciones para acceder a la información únicamente por personas autorizadas definidas por la alta dirección de la empresa.

Integridad. Hace referencia a la importancia de mantener la información libre de modificaciones y el cumplimiento de ciertas normas para operar con ella de parte del personal autorizado por la empresa.

Disponibilidad. Hace referencia a la importancia que implica disponer de la información por parte de los usuarios o procesos autorizados en el momento que se requiera, (Escrivá et al., 2013) mencionan que ningún sistema es seguro al 100%, por ello elevar los niveles de seguridad debe ser una preocupación constante, evitando así poner en riesgo cualquiera de los principios básicos de nuestra información.

No repudio

Según Álvarez & Pérez (2004) afirma que el no repudio busca reunir, mantener, hacer disponible y validar una evidencia irrefutable en relación a un suceso o acción con el fin de resolver disputas acerca de la ocurrencia o no de dicho suceso o acción.

El no repudio es un servicio típicamente ofrecido por un medio garante adjuntado a los datos, ya que debido a la imposibilidad de ser falsificada testimonia que el usuario, y solamente él, pudo haber realizado la transacción (p.150). El no repudio trata de prevenir que un emisor niegue su participación en una transacción, es por esto que, contar con este servicio resulta muy importante para aumentar la confiabilidad de las acciones realizadas y sus autorías.

Conceptos básicos de seguridad

- **Activo**

En el contexto empresarial, los activos que posee una organización tanto tangibles como no tangibles, son muy importantes y merecen un tratamiento especial.

Un activo se define como aquel recurso del sistema (informático o no) necesario para que la organización alcance los objetivos propuestos, es decir, todo aquello que tenga valor y que deba ser protegido frente a un eventual percance, intencional o no. Según esta esta definición, se considera como activos: el software, los datos, los archivos, el hardware, las comunicaciones, entre otros. (Escrivá et al., 2013, p. 8)

Es todo aquello que posee una organización y considera que tiene un valor especial, ya que de algún modo es requerido para el logro de sus objetivos, por ello debe ser protegido efectivamente.

- **Vulnerabilidad**

Son fallas que pueden encontrarse en todo tipo de software, y es importante su prematura detección por parte de los responsables y de esta forma encontrar soluciones para corregirlas.

En la mayoría de casos estos responsables son desarrolladores de software o administradores de seguridad y trabajan en pronta aplicación de estas correcciones, buscando prevenir la divulgación de las vulnerabilidades, ya que de no hacerlo se corre un gran riesgo de ser aprovechadas por ciertos individuos que accedan a los sistemas (Portantier, 2012, p. 177).

Cuando las vulnerabilidades son detectadas, deben ser corregidas inmediatamente con la finalidad de prevenir ataques, de este modo se evitarán riesgos innecesarios que puedan comprometer a la información.

- **Amenazas**

Se considera amenaza a cualquier entidad o evento que afecte el funcionamiento de un sistema informático que pueden ser voluntarias o involuntarias. Estas amenazas suelen dividirse en dos tipos: amenazas pasivas, que buscan obtener información a través de una comunicación y por otro lado las amenazas activas que buscan realizar cambios en el estado de sistemas de forma no autorizada (Escrivá et al., 2013, p. 9). Una amenaza puede ser representada por medio de una persona, evento, circunstancia o fenómeno que provoque efectos negativos en los sistemas de información, ocasionando pérdidas y daños significativos de todo tipo.

- **Ataque**

Un ataque es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él, incluso tomar control del mismo. Se

trata de acciones intencionadas como fortuitas que pueden llegar a poner en riesgo a un sistema (Escrivá et al., 2013, p. 9).

En pocas palabras puede determinarse a un ataque como una actividad producida por un evento natural o provocado, la cual hace uso de una debilidad dentro del sistema generando un impacto negativo.

- **Riesgo**

Riesgo es el resultado del análisis de vulnerabilidades, amenazas, grado de exposición y probabilidad de explotación sobre sistemas que pueda afectar las estaciones de trabajo. Generalmente estos riesgos se categorizan en bajos, medios y altos (Portantier, 2012, p. 39). En otras palabras, no es más que la probabilidad de ocurrencia de un incidente de seguridad a través de una amenaza, valiéndose de alguna vulnerabilidad.

- **Impacto**

Es el grado de afectación o consecuencias sobre el funcionamiento regular y proceso productivo de una organización producido por la materialización de una amenaza. Las consecuencias para todas las empresas no son iguales, en algunos casos unas adoptan estrategias de respuesta y medidas preventivas, minimizando de esta forma el impacto negativo que generaría la materialización de alguna amenaza, teniendo en cuenta que el nivel de impacto, ya que mientras más grande es su afectación, las consecuencias también lo son. Por todo ello, la identificación de impactos debe ser una tarea a realizar dentro de los objetivos del análisis de riesgos en las organizaciones (Escrivá et al., p. 13).

Control de Acceso

Gómez (2014) sostiene que mediante el control de acceso a los distintos recursos del sistema es posible implementas las medidas definidas por la organización, teniendo en cuenta las restricciones de acceso a las aplicaciones, a los datos guardados en el sistema informático, a los servicios ofrecidos (tanto internos como externos) y a otros recursos de tipo lógico del sistema (..). El modelo de seguridad aplicado en el control

de acceso se basa en la definición y gestión de determinados objetos lógicos (dispositivos lógicos, ficheros, servicios) y sujetos (usuarios y grupos, equipo, procesos, roles) a los que se conceden derechos y privilegios para realizar determinadas operaciones sobre objetos. Estos derechos y privilegios se pueden verificar mediante el proceso de autorización … (p, 110)

Fundación Telefónica (2016) menciona que en todas las organizaciones existen zonas donde se almacena información confidencial o de suma importancia. Por eso es recomendable implementar una serie de políticas de control sobre quiénes podrán acceder a los activos críticos para minimizar el riesgo, y esto se realiza mediante las herramientas que nos ofrecen el control de accesos y la gestión de identidades. Para la correcta gestión de los controles y las identidades, es necesario llevar a cabo acciones de inventariado y catalogado y establecer los criterios de acceso. Estos criterios de acceso deben regirse por la máxima de que una persona debe tener disponibilidad de las aplicaciones críticas o zona restringida solo cuando el ejercicio de su trabajo lo requiera. (pp. 21-22)

El control de acceso abarca el proceso de autenticación, es decir se encarga de verificar la identidad de los usuarios, donde está configurado especialmente para aprobar o rechazar las solicitudes de acceso por los usuarios, dependiendo de los permisos que posea cada uno de estos y si están autorizados a acceder o no.

Para lograr la mitigación de los riesgos de seguridad presentes en una organización es imperiosa la ejecución de pruebas y lograr diagnosticar las vulnerabilidades existentes en los sistemas de información, efectuando la evaluación de las mismas y el planteamiento de estrategias de atenuación de los riesgos hallados para la prevención y mejora de la seguridad en el control de acceso. (ISO/IEC 27002).

Gestión de cuentas de usuarios

Según Gómez (2014) la gestión de cuentas de usuarios constituye un elemento fundamental dentro de las políticas de seguridad de la organización, ya que de ella dependerá el correcto funcionamiento de otras medidas y directrices de seguridad

como el control de acceso lógico a los recursos o el registro de actividad de los usuarios (p, 104).

Poder llevar un control detallado de los usuarios registrados que acceden a los sistemas de información y los permisos asignados a los mismos, resulta ser una tarea mucho más sencilla si se encuentra acompañado de una correcta gestión, orientado hacia el cumplimiento de las políticas y directrices desplegado por parte de la alta dirección y responsables de su aplicación.

Autenticación de Usuarios

Autenticar es identificar a un usuario con un grado aceptable de confianza. Tradicionalmente, las distintas formas de identificar a los usuarios que intentan acceder a un recurso o servicio han girado en torno a tres métodos:

- Restringir el acceso en función de algo que el usuario conoce, como, por ejemplo, una contraseña
- Restringir el acceso en función de algo que el usuario posee, como, por ejemplo, un token USB o un certificado digital almacenado de forma segura dentro de una tarjeta inteligente (smartcard).
- Restringir el acceso en función de algo que el usuario es fisiológicamente. El método más implantado es la biometría (Álvarez & Pérez, 2004, p.146).

La autenticación es el proceso que tiene la gran labor de validar la identidad de un usuario a través de credenciales, donde los niveles de seguridad y confianza aumentan cuando dichas credenciales aseguran ser únicas e irrepetibles.

Contraseñas

Álvarez & Pérez (2004) definen que es la técnica de autenticación más utilizada por los usuarios, pero a su vez la más débil, debido a su facilidad de explotación por un atacante tras ser descubierta u obtenida. Es posible llevarse a cabo aprovechando el desconocimiento, descuido y/o irresponsabilidad de los usuarios que implica lo siguiente:

- Olvido de contraseñas o contraseñas apuntadas a la vista de todos.

- Contraseñas demasiado cortas y simples en su combinación.
- Ataques de shoulder surfing sobre las estaciones de trabajo
- Instalaciones de keyloggers involuntarios que facilite la captura de información por un sniffer.
- Ausencia en el cifrados de datos de aplicaciones y administrador de cuentas.
- Ataques de fuerza bruta entre otros (pp. 146-147).

Las contraseñas permiten que los usuarios accedan a los sistemas y recursos de forma segura, así también, ayudan a restringir el acceso a quien no esté autorizado.

Gestión de la seguridad

La información es un conjunto sistematizado de datos, que conforman una idea, para ser transformado en conocimiento apoyando a la toma de decisiones. Álvarez & Pérez (2004) la ausencia de medidas de protección influye negativamente en la seguridad de la información debido a que se encuentra expuesta a múltiples amenazas y riesgos asociados si estas se materializan. La seguridad de la información se encarga de gestionar los riesgos dentro de los sistemas informáticos a través de medidas que sean capaces de mitigar las amenazas a las que los activos de una organización están expuestos. La gestión de la seguridad se resume en la aplicación e integración de políticas, estándares, mecanismos y procedimientos de seguridad con el objetivo de asegurar la información y demás activos de una organización.

Procedimientos de seguridad

Estos documentos provienen de los estándares de seguridad sirviendo de guías, en los se detalla de forma práctica las tareas a realizar por todos los miembros de la organización sin importar su grado de experiencia ante cualquier eventualidad. (Portantier. 2012, p. 49).

De acuerdo a lo anterior, son los principales responsables en el establecimiento de necesidades y requisitos en el entorno organizacional para definir un plan de seguridad que represente gráficamente el sistema de seguridad informática diseñado, y en base

a ello, utilizar los procedimientos más adecuados en función a las acciones y tareas a realizar.

Planes de contingencia

Un plan de contingencia está conformado por una serie de medidas pertinentes a utilizar en caso que un sistema falle o se desee recuperarlo, este debe ser revisado continuamente para su adaptación a las necesidades de la organización. En él se considera las siguientes fases:

Evaluación, fase de creación del grupo que desarrollara el plan, identificación de activos a proteger, su impacto si hubiera daños y posibles soluciones.

Planificación, fase en la que se documenta y validad el plan por los responsables o áreas envueltas a través de pruebas de viabilidad y ejecución.

Recuperación, fase en la que se pretende restablecer el orden tras la ocurrencia de un ataque o incidente (Escrivá et al., 2013, p. 17).

Un plan de contingencia debe contemplar todos los elementos intervinientes en los sistemas, como datos, documentación, hardware, software, personas; en base a lo anterior, diseñar un plan de acción bajo una estrategia considerando los recursos disponibles para combatir los posibles problemas que puedan presentarse y aplicar la solución más óptima.

Análisis de riesgos

Álvarez y Pérez (2004) afirman que el análisis de riesgos de los activos que se pretende proteger es una de las actividades iniciales a realizar incluida en la etapa de planificación de la seguridad de la información, por tener el propósito de identificar los riesgos existentes, medir su impacto y apreciar su costo de mitigación.

El análisis de riesgos es aquel proceso que se encarga de identificar los activos informáticos, como sus vulnerabilidades, amenazas a las que están expuestas, así mismo, la probabilidad de ocurrencia e impacto de las mismas. Su objetivo es determinar los controles correctos que aporten para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Registro de fallos

Un registro detallado de los problemas encontrados en los sistemas, tales como amenazas, vulnerabilidades, detección de intrusos entre otros puede ser muy útil para el área o persona responsable. Oficina Nacional de Tecnologías de Información (2005) el ente responsable deberá desarrollar y verificar que se cumpla con los procedimientos y se comunique inmediatamente las fallas que se presenten para sus respectivas correcciones, en ella deberá incluir lo siguiente: revisión de registro de fallas, revisión de medidas correctivas y su respectiva documentación (p. 47).

Cuando se presentan fallos en los sistemas de información, la mejor forma de afrontarlas es registrarlos, un registro detallado de ellos permitirá tomar acción inmediatamente para evaluar sus características y comportamientos que determinen los procedimientos más adecuados para su mitigación.

Amenazas a la seguridad de la información

Según Álvarez & Pérez (2004) se conoce como malware a todo aquel software maligno para los sistemas informáticos, el cual guarda relación con los siguientes términos dentro del mundo digital.

- **Malware,** ante el inminente crecimiento tecnológico y digital a nivel mundial es imprescindible para todas las organizaciones resguardar la información que posee sobre sus recursos informáticos.
- **Virus,** programas dañinos, archivos ejecutables característicos por replicarse en los sistemas y demás archivos.
- **Gusanos,** fragmentos de código replicables en una red automáticamente aprovechándose de vulnerabilidades o desconocimiento de usuarios.
- **Troyanos,** programas con puertas traseras invocadas por los intrusos (pp. 39-40).

Estos tipos de software maliciosos tiene como objetivo infiltrarse en los sistemas informáticos sin permisos del propietario y en muchos casos sin conocimiento del mismo, comprometiendo tanto a la información como los recursos propios del sistema, afectando el correcto funcionamiento del mismo.

Mecanismos de seguridad

Un sistema protegido requiere de un análisis profundo, sobre todo potenciales amenazas que puedan comprometerlo, además de la probabilidad que ocurra. A partir de este punto se define la política de seguridad que defina responsabilidades y las reglas para minimizar los efectos de amenazas que puedan ocurrir. Los mecanismos de seguridad se dividen en mecanismos de prevención, mecanismos de detección y mecanismos de recuperación (Huidobro & Roldan, 2005, p. 11).

Los mecanismos de seguridad son utilizados como técnicas o elementos de fortalecimiento para la confidencialidad, la integridad y/o disponibilidad de un sistema informático. Estos mecanismos varían y su elección depende de ciertos factores como funcionalidad, niveles de riesgos, tipos de amenaza, entre otros elementos.

Administración segura

La administración segura es considerada una buena práctica dentro de la seguridad informática, pero una de las más difíciles de implementar por los administradores, debido al excesivo uso del usuario administrador ya sea por comodidad o costumbre. Este accionar genera una serie de riesgos asociados, lo cuales resultan en la concesión de privilegios al verse comprometido por algún proceso. Un punto clave es gestionar los parches, horfixes y actualizaciones; entrando a un nivel más técnico el hardering de servidores, con el objetivo de elevar los niveles de seguridad a través de configuraciones en las que se incluye por lo general la deshabilitación de servicios y funciones que estén en desuso. (Benchimol, 2011, p. 22). De acuerdo a lo anterior, consiste en el reforzamiento de la seguridad lógica sobre los recursos informáticos llevada a cabo por los administradores, donde el principal objetivo es configurar adecuadamente los servicios y funciones, gestionando las actualizaciones de las aplicaciones en los sistemas.

Ingeniería Social

Según Gómez (2014) “Se ha adoptado el termino de Ingeniera Social (Social Engineering) para referirse al conjunto de técnicas y trucos empleadas por intrusos y

hackers para extraer información sensible de los usuarios de un sistema informático …" (p, 132).

Escrivá et al. (2013) afirman que la ingeniería social es una forma de fraude informático muy utilizado por piratas informáticos y consiste en manipular el comportamiento natural de los usuarios mediante engaños y mentiras.

Los argumentos utilizados son muy convincentes y conviene estar muy alerta. Para extender estas estafas o fraudes, los atacantes utilizan una gran variedad de herramientas o técnicas. (p. 121)

La ingeniería social es un tipo de ataque donde los individuos a través del arte del engaño y la manipulación psicológica de las personas logran extraer información de ellas utilizando diversos medios de comunicación.

Amenazas del personal interno

Según Gómez (2014) se debe considerar el rol que desempeña el personal en los diversos incidentes de seguridad y ataques posibles de manera consciente o inconsciente. Y de este modo poder identificar en el personal aquellos comportamientos o motivaciones propias que puedan poner en riesgo a la organización y conlleve a efectos negativos, es por ello, que resulta imprescindible fortalecer la seguridad en los sistemas informáticos en relación a los empleados (usuarios tanto internos como externos).

Tipos de Ingeniería Social

Phishing

Es un término informático, que a través de la ingeniería social se pretende obtener información confidencial de forma engañosa. Los phishers, quienes utilizan esta técnica se hacen pasar por otra persona o entidad de confianza, imitando y simulando sus características de forma creíble.

Este tipo de ataque se lleva a cabo a través de medios digitales o de comunicación con el objetivo de acceder a información relevante de la víctima como podría ser contraseñas, información de usuarios entre otros (Jara & García, 2015, pp. 300-301).

El phishing es una técnica de suplantación de identidad en donde un atacante se hace pasar por una entidad o persona de forma creíble, llevándolo a cabo por medio llamadas telefónicos o envió masivo de correos electrónicos, informando la indisponibilidad de un servicio a causa de un problema, y solicitando las credenciales de usuario para su solución, capturando toda la información ingresada por el usuario.

Ataques de fuerza bruta

Según Jara & García (2012) este tipo de ataques tiene como objetivo comprometer la seguridad en mecanismos de autenticación que se basen en el uso de clásico de credenciales (usuario y contraseña), a través del ingreso múltiple de claves y combinaciones posibles que permitan el acceso a un sistema.

Un ataque de fuerza bruta es un tipo de ataque básico que no requiere de software ni recursos informáticos automatizados, se basa solamente en que el atacante pruebe contraseñas con todo tipo de combinaciones hasta lograr dar con la correcta.

Office Snooping

Esta técnica se basa en el aprovechamiento de la ausencia de cualquier colega en su estación de trabajo con la finalidad de recabar información sobre sus terminales, facilitando el trabajo del atacante si es que no se bloquearon efectivamente las sesiones antes de abandonar su puesto temporalmente. Las ventajas que el atacante puede sacar de esto van desde recopilación de información, manipulación de archivos y accesos a aplicaciones corporativas no autorizadas hasta la instalación de programas maliciosos. Adicionalmente debe ponerse mayor atención en cuanto a privilegios de usuarios, al tipo de información que se gestiona y los medios que permiten su difusión de forma integral, ya que un medio comprometido podría ser el punto de partida para que los demás también lo sean (Ramos, Barbero, Marugán & González, 2015, p. 38).

En referencia a lo anterior, office snooping es un tipo ataque de ingeniería social en el cual un individuo aprovecha algún descuido por un compañero en su estación de trabajo y en su ausencia tomar su lugar logrando acceder al sistema, y de esta forma realizar acciones que puedan comprometer a la información.

Dumpster diving o trashing

El dumpster diving o trashing se basa en la búsqueda de información útil como memorias, documentos, contraseñas entre otros en medios donde se acumulan desechos, dicha información podría ser aprovechada posteriormente por un ingeniero social, es por ello que en diferentes países las autoridades prohíben buscar entre los desechos, ya que encontrar información relevante en ellos no se descarta y las razones son principalmente por negligencia de quienes la custodian o mala intención (Ramos et al., 2015, p. 30-31). Generalmente, este ataque se manifiesta en la búsqueda relevante de información en los desechos, aprovechándose de la falta de conciencia y descuido de algunos empleados por deshacerse de documentos o alguna otra información sin destruirla previamente.

Shoulder Surfing

Es considerada una de las técnicas más clásicas con respecto a la recolección de información relevante, la cual se basa en la observación directa, pero de manera disimulada por parte del atacante con el fin de obtener contraseñas o cualquier otro tipo de información por parte de la víctima. Estas acciones pueden realizarse en cualquier lugar mientras la victima ingrese sus credenciales de acceso en algún dispositivo de su preferencia. Además, el avance tecnológico hoy en día permite la existencia de métodos más sofisticados que involucran el uso de dispositivos de observación avanzada facilitando de manera significativa esta labor a los atacantes (Ramos et al., 2015, pp. 36-37). Es necesario recalcar que es una técnica basada en la observación, donde un atacante pretende obtener las credenciales de acceso de los usuarios o cualquier tipo de información que puede ser de utilidad en un posterior ataque.

Ingeniería inversa

Esta modalidad a diferencia de otras opera de forma pasiva, es decir en sentido inverso, donde lo que se busca es que la víctima sea quien se dirija a su atacante y no al revés, es por ello que se considera una de las modalidades más exitosas. Puede llevarse a cabo de forma dirigida o colectiva utilizando diversos medios como redes

sociales, correos electrónicos, llamadas telefónicas, sitos webs e incluso personalmente, timando a su víctima para que este dé el primer paso sin darse cuenta. Esta modalidad es el punto de partida que conduzca a un ataque de ingeniería social exitoso a futuro (Ramos et al., 2015, pp. 39-40).

Motivaciones y causas

Toda aquella información que brinde beneficios y ventaja competitiva a una empresa frente a las demás será blanco del espionaje corporativo los cuales pueden ser planes, estrategias e incluso secretos, que en manos equivocadas pueden ser manipulada de diversas formas afectando negativamente a la empresa propietaria. Por ello, toda aquella información confidencial resguardada por una empresa que le otorgue buenos resultados, será el punto de partida para llevar a cabo espionaje corporativo (Jara & García, 2015, pp. 30-31).

Las motivaciones de un atacante para realizar ingeniería social pueden ser diversas, desde subvenciones económicas por espionaje y robo de información hasta motivaciones personales, como acciones que perjudiquen a un empleado o a la misma empresa.

Desconocimiento y falta de sensibilización del personal

La implementación de soluciones tecnológicas como principio básico de seguridad son inútiles ante la ignorancia, desmotivación, deslealtad o mala fe por parte de los empleados, por esta razón, es que en la mayoría de casos que se presentan relacionados a problemas de seguridad en las organizaciones el factor humano es el principal responsable.

La ausencia de concientización a los colaboradores acerca de mantener la información segura, el debido uso de las herramientas para este fin y lo que ello implica como consecuencias e impacto recae en la responsabilidad sobre la alta dirección, por lo que es conveniente desplegar el compromiso y sensibilización sobre estos temas a todos los colaboradores (Gómez, 2011, p. 179).

Desconocimiento y falta de sensibilización del personal en temas de seguridad son los principales problemas en las organizaciones, debido a que el contar con todo tipo de

política, procedimientos, normas y sistemas de seguridad, no garantiza absolutamente, si el talento humano no está debidamente capacitado y concientizado en estos temas.

Insider

Es aquel individuo dentro de la organización que tiene ciertos privilegios y accesos autorizados a información confidencial, el cual puede realizar ataques internos difíciles de detectar y facilitando luego información a terceros de forma sencilla utilizando por ejemplo la estenografía. Sus motivaciones pueden ser variadas ya sea a causa de competitividad empresarial, problemas laborales, asuntos personales o lucrativos.

Sin embargo, también pueden existir insiders no intencionado o involuntario que represente una amenaza a la organización siendo víctimas de actividades de forma consciente o inconsciente, es por todo esto que los ataques de son considerados por las organizaciones como uno de los más peligrosos que existen (Ramos et al., 2015, p. 21)

Un insider es aquella persona que labora en una organización y que cuenta con ciertos accesos a sistemas de información para el desarrollo de sus actividades, y que, valiéndose de esos permisos, puede generar daños que comprometan a la organización, sin embargo, pero también existen insider no intencionados que de igual forma representan una debilidad al ser blanco de ataques futuros.

Fallos humanos

Es de suma importancia integrar esfuerzos en la formación del factor humano respecto a temas de seguridad involucradas en el desarrollo de sus actividades, dado que el factor humano es el elemento más importante dentro de un sistema informático, pero a la vez el más vulnerable.

Los distintos ataques de ingeniería social pueden aprovechar perfectamente los distintos fallos humanos facilitando la labor del atacante. Por ello, se recomienda prohibir a los empleados el uso de correos electrónicos y herramientas colaborativas propias de la empresa para usos ajenos al trabajo, asimismo, sensibilizar y formar al

factor humano sobre seguridad informática, con la finalidad de mantener protegidos los activos custodiados (ACISSI, 2015, p. 54).

Los fallos humanos en una empresa representan una de las mayores amenazas a la seguridad de la información, puesto que en muchas ocasiones el personal no cuenta con la formación debida en estos enfoques, y desempeñan sus actividades erróneamente, siendo el blanco de cualquier ataque capaz de aprovecharlo.

Conspiración y coacción

La detección de amenazas externas permite tomar acciones inmediatas para controlarlas, sin embargo, pueden encontrarse amenazas internas difíciles de detectar. Solé (2013) los ataques de conspiración son realizados por usuarios autorizados que podrían facilitar el acceso al sistema motivados probablemente por temas de soborno, por otro lado, la coacción se manifiesta a través de una víctima por chantaje o amenaza facilitando el acceso al sistema a alguien. En ambos casos la seguridad es burlada debido a que dichos ataques son realizados con credenciales reales (p. 10). Tanto la conspiración como coacción son ataques en los que necesariamente interviene un usuario autorizado, la diferencia reside en que un ataque de conspiración induce a la víctima en su accionar de forma voluntario, en cambio, la coacción somete en su accionar a la víctima dejándole pocas opciones de elección.

Espionaje corporativo

Nace junto a la revolución industrial, debido a los secretos productivos por parte de las empresas, los cuales fueron la clave del éxito en su negocio y por cuya razón las empresas guardaban celosamente. En este escenario, las empresas intentaban conseguir información valiosa de diferentes formas que les permitiera alcanzar ventaja competitiva frente a la competencia. De esta manera, lograban posicionarse por encima de aquellas que no disponían de dicha información.

Es así que nacen los espías industriales, con el objetivo principal de obtener información a través de métodos poco éticos y legales. Al tratarse de un bien no tangible el robo de información puede ser más sencillo, presentándose casos en los que la empresa victima ha sido afectada por largo tiempo sin darse cuenta. Estas

acciones resultan ser una amenaza en manos de la competencia convirtiéndose en conocimiento que puede volverse en contra de aquellas empresas afectadas.

Cabe la posibilidad de que espías profesionales generen su vector de ataque a través de descuidos y actividades no controladas realizadas dentro de la organización como, conversaciones privadas, documentos desechados, proyectos y restos de materiales de viajes, entre otros (Benchimol, 2011, p. 30).

El espionaje corporativo consiste en la ejecución de acciones orientadas a la sustracción de secretos comerciales de otras empresas por medio de la infiltración (espionaje), el cual es muy difícil de detectar. También puede ser provocado por reacciones de los empleados a cambios en la compañía, así mismo incluye la obtención de información sobre empleados con cargos importantes o altos ejecutivos.

Ex-empleados

Escrivá et al. (2013) afirman que aquellos empleados que ya no forman parte de su centro de labores. podrían tomar acciones de represarías contra el mismo, siendo motivados por sentimientos como el despecho o la venganza, aprovechando en ciertos casos el contar aún con sus credenciales de acceso a los sistemas de información de la organización, los cuales debieron haber sido dados de alta desde el momento en el que dejaron de formar parte de la misma. Así también diversos daños que impliquen que la información pueda verse comprometida.

Las decisiones administrativas como reducción de personal o separación de sus funciones de empleados por diversas razones, pueden sufrir repercusiones futuras en función a la relación empleado-empresa, ya que podría ser el motivo perfecto para que el ex-empleado aproveche ciertos privilegios que aún no han sido dados de baja, a merito que le permita acceder a información y tome acciones en contra de su ex centro de labores.

Espías

Por razones obvias, el personal involucrado en tareas de espionaje privado o gubernamental usa ingeniería social para hacerse pasar por otros o para manipular a sus objetivos, ello en virtud de realizar determinadas acciones en su beneficio.

También es habitual la representación de diferentes papeles o leyendas con el objetivo de obtener información o infiltrarse en el entorno que les sea de interés. (Escrivá et al., 2013, p. 23).

El rol de los espías básicamente tiene el objetivo recabar información y brindarla a quienes lo contrataron para este fin, utilizando técnicas de ingeniería social para infiltrarse sin levantar sospechas en la organización víctima.

Intrusos remunerados

En este sentido, sin duda alguna, es el tipo de amenaza con mayor peligro, pero a su vez el menos habitual. Escrivá et al. (2013) mencionan que aquellos que son intrusos que son remunerados, son especialistas en informática manteniendo contrato con una tercera persona o entidad con el objetivo de extraer y apoderarse de información sensible.

Son individuos pagados por una tercera parte con el fin de robar secretos (información confidencial) o causar daños que repercutan de alguna forma la imagen de la entidad atacada.

Formación del personal

Portantier (2012) refiere que se sabe que el personal responsable de la seguridad informática debe de mantenerse actualizada y capacitada constantemente ante los nuevos paradigmas de seguridad. Pero muchas veces se descuida este aspecto y los incidentes de seguridad que surgen son a causa de negligencia de los usuarios y la responsabilidad recae en los responsables de la organización por no prever que tan importante es capacitar adecuadamente a sus miembros.

Por ello, son muy importante los programas de capacitación que estén a disposición de los usuarios, y que posteriormente se evalué, para verificar que los conocimientos adquiridos fueron comprendidos, asimismo, persistir en la difusión constante de recomendaciones y consejos de seguridad para que lo tengan en cuenta en todo momento. (pp. 53-54)

La formación del personal debe ser una actividad frecuente y un compromiso integral por parte de los miembros de toda organización que pretendan mantener o elevar la productividad de sus procesos, pero sobre todo mantener seguro sus activos. Tener colaboradores capacitados, reducirá significativamente riesgos que puedan comprometer los activos de la organización.

Políticas de Seguridad

Según Álvarez & Pérez (2004) la implantación de políticas de seguridad en una empresa resulta ser una de las mejores maneras de cubrir las expectativas de la organización al ser desplegadas para su cumplimiento, así como las consecuencias de hacerlo y no hacerlo. Además de definir el alcance, áreas, responsables y recursos involucrados, permitiendo tener una visión más amplia y detallada que facilite aplicar los procedimientos correspondientes ante cualquier tipo de evento. Es el punto de partida para su desarrollo, que debe estar alineado de forma clara a los objetivos que la organización persigue, teniendo en cuenta todos los elementos integrados en los procesos, personas, recursos, herramientas e información.

Estándares de seguridad

Los estándares de seguridad documentan la forma en como la organización alcanzará sus objetivos respecto a la seguridad, adicionalmente la manera cómo responderá a los problemas y toma de decisiones. Por lo general, son generados por entidades externas y adoptados parcial o totalmente por la organización, en ellos se describen diferentes puntos y se exponen las estrategias de la organización, las cuales deben estar alineadas a las políticas ya que estas serán el punto de partida para la redacción de los procedimientos (Portantier, 2012, pp. 48-49). Es por ello que los estándares de seguridad cumplen un rol de guías y buenas prácticas, proporcionando información sobre la gestión de la seguridad de la información y el modo de operación.

Norma ISO 27001

La norma ISO 27001 es un estándar internacional orientado a la seguridad de la información, el cual explica cómo implementar un sistema de gestión de la seguridad en las organizaciones, las cuales definen las medidas de seguridad aplicables en los

sistemas de información, garantizando su protección por medio de infraestructuras de almacenamiento en la nube y mejora continua (Auditoría, Consejo, Instalación y Seguridad de Sistemas de Información, 2015, p. 410). Estos lineamientos permiten reducir posibles riesgos en los sistemas informáticos y de información a nivel global, además de aportar mejoras en procesos y servicios, aumentando competitividad y asegurando, la confiabilidad, integridad y disponibilidad de la información tanto del personal como de los clientes.

Auditoria Informática

Resulta indispensable para una organización conocer la situación actual por la que pasa respecto a los niveles de seguridad en sus sistemas de información.

La auditoría constituye uno de los servicios de seguridad básicos para mantenerse informado en todo momento de lo que está sucediendo o ha sucedido en el sistema. Gracias a los registros de actividad (logs), el administrador puede saber cuándo y cómo fue atacado un sistema y qué porciones fueron atacadas. (Álvarez & Pérez, 2004, p. 150)

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias que determinen si un sistema de información cumple con salvaguardar empresariales, mantener la integridad de los datos y uso eficiente de sus recursos.

Objetivos de una auditoria de seguridad

La definición de los objetivos en una auditoria informática es definida previamente a su ejecución en los cuales se incluyen una serie de términos y condiciones entre el cliente y auditor.

ACISSI (2015) el objetivo es medir los niveles de seguridad y acceso a la información de sistemas informáticos con el fin de proteger la integridad, confidencialidad y disponibilidad de los activos. Este se lleva a cabo bajo un entorno de pruebas en condiciones reales controladas simulado ser un atacante y así comprender como piensa, tomando esa posición para defenderse de mejor forma. (p. 32).

Los principales objetivos de una auditoría informática se resumen en controlar el funcionamiento y análisis eficiente de los sistemas informáticos, asimismo, verificar el cumplimiento de normas establecidas y revisar eficazmente la gestión global de los recursos informáticos.

Evaluación de seguridad

Este proceso tiene el objetivo de evaluar los niveles de seguridad en sistemas, infraestructura, comunicaciones que la organización dispone, para lo cual se requiere el uso de actividades de mejora continua, valiéndose de pruebas de intrusión que permitan detectar y explotar vulnerabilidades para que de este modo se puedan desplegar los procedimientos de seguridad y contramedidas oportunas. (González, 2014, p. 23).

La evaluación de la seguridad es aquel proceso que permite medir el grado de seguridad de la información en las empresas a través de pruebas y simulaciones de ataques en entornos controlados y aplicar así las soluciones oportunas a los problemas encontrados.

Tipos de Auditoria Informática

Auditoria de caja blanca

La auditoría de caja blanca se enfoca en el rol de un usuario interno de la organización o empresa, el cual dispone de acceso a los sistemas internos o a la totalidad o parte de los datos críticos de esta. En este tipo de auditorías se revisan configuraciones de sistemas, políticas, y servicios, código de aplicaciones, con el fin de encontrar puntos críticos que permitan a los usuarios con cierto grado de privilegios obtener acceso. El entorno empresarial puede ser esquema complejo y foco de vulnerabilidades que, aunque no se ven, existen. Es importante la realización de este tipo de auditorías para comprobar lo que un usuario con ciertos privilegios puede llegar a lograr.

Auditoria de caja negra

La auditoría de caja negra permite al auditor tomar el rol de un hacker, el cual no conoce ninguna característica del interior de la empresa o la organización. En otras

palabras, la visión global del sistema es ciega, ya que no se conoce como se organiza interiormente de los sistemas y redes. El auditor se encargará de recopilar todo tipo de información sobre el objetivo, esta información es pública después ira tomando contacto con los sistemas y servicios públicos de la empresa objetivo.

Auditoria de caja gris

La auditoría de caja gris permite al atacante tomar el rol de un cliente, un empleado con pocos o ningún privilegio, un empleado de una ubicación concreta, por ejemplo, un empleado de finanzas. El auditor disponible de una visión “a medias” de los sistemas, se encuentra dentro de la empresa, pero no dispone del mismo nivel de acceso que en la caja blanca. Es por lo tanto un empleado descontento que intenta acceder a la información a la que no tiene acceso, simulando el ataque interno a la empresa (González, 2014, p. 19).

Mencionado lo anterior, podemos clasificar las auditorias de seguridad en 3 tipos.

La auditoría de seguridad de caja blanca en la que se facilita mayor información a nivel técnico respecto a las demás auditorías, como especificaciones sobre los activos que serán auditados e información adicional como usuarios, contraseñas, mecanismos de seguridad entre otros. Toda esta información suministrada por la organización al auditor será de vital importancia y consideración en el desarrollo de su trabajo y documentación pertinente.

La auditoría de seguridad de caja negra en la que el auditor no posee conocimientos de la infraestructura tecnológica debido a que la organización no le brinda ningún tipo de acceso o información al auditor. Este tipo de auditoria es idóneo para simulaciones de ataques externos a la organización y de este modo conocer el nivel de exposición ante un ataque.

Y finalmente, la auditoria de seguridad de caja gris donde se le brinda al auditor cierta información y privilegios como si fuese un cliente o empleado de la empresa que se va a auditar, dichos privilegios y accesos serán de gran ayuda en el desarrollo del proceso de auditoria con la finalidad de que el auditor trate de escalar privilegios a partir de lo que se le brindo previamente.

Tipos de hackers

Hackers

Benchimol (2011) afirma que la palabra hacker es un neologismo, que en informática se utiliza para referirse a un gran experto en algún área de dominio. Si bien lo relacionamos más con los conocimientos técnicos e informáticos, es posible extender el concepto hacia otras disciplinas. De esta manera, definimos a cualquier persona a la que le apasiona el conocimiento, el descubrimiento, el aprendizaje y el funcionamiento de las cosas. (p. 14-15)

Un hacker es individuo apasionado por la seguridad con conocimientos en informática, que está en la capacidad de vulnerar sistemas informáticos, pero sin cometer actos delictivos después de lograr acceder a estos.

Crackers

Benchimol (2011) afirma que el término cracker proviene del vocablo inglés crack (romper). Aplicado a la informática, podemos decir que es alguien que viola la seguridad de un sistema de forma similar a un hacker, solo que ilegalmente y con diferentes fines. También se aplica específicamente al software: denotando a aquellas personas que utilizan la ingeniería inversa sobre éste, con el objetivo de desprotegerlo, modificar su comportamiento o ampliar sus funcionalidades originales. (p. 17)

Un cracker es individuo con conocimientos en informática que, a cambio del hacker ético, este busca vulnerar los sistemas informáticos ilícitamente y sacar el mayor provecho posible de ello. También suelen ser llamados piratas informáticos o ciberdelincuentes.

Los hackers black hat

ACISSI (2015) afirma penetran rompiendo los sistemas, con un interés que no es el mismo que el de los propietarios de la red o del sistema, sino más personal y/o lucrativo. En este grupo, están los crackers, que sienten una fuerte atracción hacia este lado oscuro. Los crackers son por ejemplo el origen de los virus, los troyanos y el

spyware. Cuando se realiza este tipo de acciones con el propósito de dañar a una organización o a personas, se habla también del terrorismo, o ciberterrorismo. (p. 34)

Los hackers black hat son quienes utilizan su conocimiento para ingresar en los sistemas informáticos saltándose la seguridad de los mismos como lo hacen los hackers white hat, solo que, de una manera maliciosa, buscando económicos y personales.

Los hackers white hat

ACISSI (2015) afirma que un hacker white hat analiza los sistemas informáticos para descubrir vulnerabilidades todavía no conocidas o sin publicar, las “0 day” (cero day, día cero). La técnica empleada es la misma que la empleada por un hacker black hat. La diferencia entre ambos radica en sus acciones desde el momento en que se descubre la vulnerabilidad.

La pregunta que surge es si hay que publicar la vulnerabilidad o no. Los hackers White hat abogan por divulgar completamente la vulnerabilidad descubierta, lo que en ingles se llama full disclosure, mientras que los hackers black hat prefieren restringir el acceso a esta información y no darla a conocer. (p. 35)

Los hackers white hat son quienes utilizan sus conocimientos para encontrar vulnerabilidades en los sistemas informáticos, y luego reportarlas para conocimiento de la compañía que lo contrato, con el objetivo de buscar soluciones y corregir estos fallos.

Los hackers gray hat

ACISSI (2015) afirma que el hacker sombrero gris es una especie de hibrido del sombrero blanco y del de sombrero negro. Se trata de un hacker competente, que actúa a veces con el espíritu de un white hat pero con una filosofía de divulgación distinta.

Su intención no es necesariamente mala, aunque de vez en cuando comete algún delito. Muchos hackers que se autodenominan white hat en realidad parecen más bien

grey hat, ya que sin dar tiempo al responsable para que corrija el problema divulga los fallos, lo que puede dañar seriamente al sistema en cuestión.

Marco legal

Benchimol (2011) menciona que, en el último tiempo, se ha prestado especial interés en el ámbito internacional y se ha llegado a un consenso en las valoraciones político-jurídicas de los problemas asociados al mal uso de un equipo informático, lo cual hizo que, en algunos casos, se modificaran los derechos penales nacionales e internacionales.

En particular, la Organización de las Naciones Unidas señala que, cuando los problemas llegan al ámbito internacional, se amplifica su magnitud y los delitos informáticos se constituyen en una forma de crimen transnacional. Respecto a qué considera como delitos informáticos, propone la siguiente segmentación:

- **Fraudes cometidos mediante manipulación de computadoras:** dentro de esta categoría, podemos citar ataques que tengan como objetivos la manipulación de los datos de entrada, de los datos de salida, de programas o el fraude efectuado por medio del mal manejo informático.
- **Modificación de datos de entrada:** en esta categoría, podemos hacer, a su vez, dos divisiones: cuando la manipulación se realiza con el objeto de modificar datos almacenados en forma digital en determinado equipo, o bien cuando se manipulan datos para falsificar documentos de uso comercial.
- **Daños o modificaciones de programas o datos digitalizados:** en esta categoría, contemplamos el sabotaje informático, el acceso no autorizado a servicios y sistemas informáticos, y la reproducción no permitida de programas informáticos de protección legal, entre otros. … (pp. 128-129)

El marco legal que refiere a la seguridad informática permite cubrir aspectos legales que de una u otra forma las organizaciones deben entender y adoptar a fin de alinear sus políticas y procedimientos internos a ella. Esta serie de disposiciones y regulaciones permite a toda organización tener un panorama más amplio sobre lo que está permitido y lo que no lo está, así también como las consecuencias de carácter

legal que tiene el no cumplimiento de las mismas. El marco jurídico actual con respecto a esta temática es el sostén de los pilares básicos de la seguridad informática, los cuales deben ser cubiertos por toda organización, y que a través de su cumplimiento ayudara a cubrir con los mínimos requisitos en la gestión de la información: la integridad, confidencialidad y disponibilidad.

Ataques informáticos

Un ataque informático un evento que se lleva a cabo de forma fortuita o intencionalmente aprovechándose de una o varias vulnerabilidades en los sistemas informáticos generando un impacto, y generalmente posee las siguientes fases:

- Reconocimiento. se recopila la mayor cantidad de información de la víctima.
- Exploración. se recopila la mayor cantidad de información del sistema.
- Abstención de acceso. se trata de explorar alguna vulnerabilidad detectada en las fases anteriores para realizar un ataque.
- Mantener el acceso. ya habiendo accedido se trata de mantener dicho acceso por medio de la implantación de herramientas.
- Borrar huellas. Como último paso se trata de borrar evidencias para para no ser detectado. (Escrivá et al., 2013, p. 10).

Son acciones producidas a raíz de alguna debilidad en el software o en el hardware que son detectados y aprovechados por delincuentes. Su exitosa ejecución llevada a cabo por un delincuente informático puede comprometer negativamente la seguridad de los sistemas poniendo en riego los activos.

Delito informático

Cuando hablamos de delito, lo primero que pensamos es en un acto ilegal, sin embargo, al unirlo con el termino informático la definición cambia y se orienta al mundo digital. Instituto Nacional de Estadística e Informática (2001) el delito informático engloba una serie de términos sobre actividades no licita bajo el uso de recursos y

medios informáticos, lo que propicia la necesidad de una regulación por parte del derecho que contemple dichos aspectos.

Estas actividades y comportamientos no lícitos muchas veces pasan desapercibidos dentro de las organizaciones ya sea por descoordinación administrativa o políticas mal definidas que dificultan su detección, e incluso la colaboración entre los mismos empleados y la administración valiéndose de sus credenciales, conocimiento y experiencia en su entorno laboral (p. 29).

De acuerdo a lo anterior, un delito informático encierra un conjunto de actividades intencionales que buscan algún beneficio pero que se encuentran fuera de la ley y utilizan recursos informáticos y/o digitales para su cometido.

Medidas correctivas

Las buenas prácticas y conocimientos del auditor se consideran medidas correctoras luego de la detección de diversos problemas en los sistemas. Entre las buenas prácticas para la corrección y mitigación de fallos se encuentra la resolución inmediata de los fallos encontrados en la configuración de servicios y permisos, aplicación de parches en entornos controlados sin afectar la producción de la organización, revisión periódica, mínima exposición de servicios y aplicaciones, mínimo privilegio posible, delimitación de responsabilidades y registro de actividad y aplicación de esquemas basados en la defensa en profundidad. (González, 2014, p. 207).

Dicho lo anterior, las medidas correctivas son una serie de mecanismos que se encargan de solucionar los errores cometidos o daños como consecuencia de un ataque, es decir, tienen la función de cambiar el estado del sistema a su estado original y adecuado.

Registros y logs

Benchimol (2011) menciona que los registros y logs de auditoría son una parte fundamental de todo esquema de seguridad. Lo que nos permite obtener un sistema de logs es un rastro de determinados eventos que se dieron en un momento determinado. Una característica de estos sistemas es que la grabación se realiza en

un medio de ingreso secuencial, los datos se van almacenando sucesivamente en el área seleccionada (p. 25).

Cuando se habla de registros y logs de auditoria hace referencia a la grabación secuencial en un archivo de almacenamiento de todos los acontecimientos (acciones y hechos) realizados por usuarios a lo largo del tiempo, es decir un historial de las actividades ejecutadas en el sistema.

Controles anti malware

Se debe considerar puntos importante como prohibición para utilizar software no autorizado, redacción de procedimientos con medidas de protección, instalaciones y actualizaciones constantes de software, mantener los sistemas en sus últimas versiones, revisiones periódicas de equipos y procedimientos, verificación sobre presencia de virus, documentación de procedimientos respecto a información de software malicioso y concientización del personal respecto a amenazas a la seguridad y plan de acción frente a estos. (ONTI, 2005, pp. 45-46).

Los controles anti malware permite mantener seguro los sistemas informáticos de software malicioso, el cual se enfoca en el seguimiento continuo para la implementación de soluciones eficaces que protejan la información ante tales amenazas.

Firewall

Según el Instituto Nacional de Estadística e Informática (2001) un firewall es una herramienta de seguridad para el control de acceso entre redes (internas y externas), actuando como vigilante en las mismas, siendo esta su principal funcionalidad, pero también la de proteger los activos y recursos de información dentro de las organizaciones.

Dicho de otra manera, es un sistema de seguridad que permite bloquear o consentir conexiones entrantes o salientes de un ordenador hacia el exterior, filtrando los paquetes que circulen a través de la red, estas configuraciones pueden realizarse de forma manual o automática.

Mínimo privilegio

Este principio hace referencia a que un usuario en el desarrollo de sus tareas solo deberá contar con los privilegios mínimos que requiere dichas tareas, es decir, solamente acceso a los recursos que le corresponden. Este principio genera ciertas ventajas muy interesantes como, reducir la probabilidad de que pueda explotarse alguna vulnerabilidad al tener pocos servicios y aplicaciones corriendo en el sistema además de influir positivamente en el rendimiento de los sistemas como en la detección de alguna falla para su depuración manera más rápida y sencilla (Benchimol, 2011, pp. 22-23).

En principio, todos los agentes que interactúan con un activo deben contar siempre con el mínimo privilegio necesario para el desempeño de sus tareas autorizadas, ya que si se les concede más se correría un riesgo que es innecesario.

Defensa en profundidad

Álvarez & Pérez, 2004) afirman que es una estrategia muy eficaz comúnmente utilizada en todo tipo de empresas, consiste en la defensa en profundidad, en la esperanza de que lo que un antivirus deje pasar, sea detectado por otro. Es algo parecido a la comparación entre pescar con red o con caña. Una red capturará muchos más peces que una caña. Cuanto más grande sea la red y más fina la malla, mayor el volumen de pescado capturado. (p. 301)

Es una técnica basada en una serie de capas la cual forman barreras de seguridad para los atacantes con el objetivo de dificultar el acceso a redes infraestructuras, en caso de que, si fallara cualquiera de los controles en una capa, se cuente con defensas adicionales que retengan la amenaza y minimicen las probabilidades de ser víctimas de un ataque informático.

Antivirus

Huidobro & Roldan (2005) afirman que los antivirus son soluciones de software cuya principal función es la detección y eliminación de virus informáticos y malware. Puede ser ejecutada por un usuario desde el mismo ordenador o desde la web. La acción principal de un antivirus para el cumplimiento de su función es la de comparar virus y

código malicioso en una base de datos, por lo que resulta esencial que esta se encuentre actualizada constantemente evitando así la infiltración de nuevos virus que no hayan sido detectados.

Es un software de seguridad que y una de las mejores maneras de protegernos de programas malintencionados que puedan dañar o modificar el normal desempeño de los sistemas informáticos e inclusive archivos e información sensible almacenada en ellos.

III. METODOLOGÍA

3.1. Tipo, nivel y diseño de investigación

El tipo de Investigación fue Aplicada y de nivel experimental.

La presente investigación es aplicada, debido a que el problema estaba establecido y fue reconocido por los investigadores. Se utilizó la investigación para dar respuesta al problema general y a los problemas específicos.

Según Carrasco (2007) “Esta investigación se distingue por tener propósitos prácticos inmediatos bien definidos, es decir, se investiga para actuar, transformar, modificar o producir cambios en un determinado sector de la realidad” (p. 43).

Es Experimental, debido a que se administró la variable independiente para observar y medir su efecto en la variable dependiente en base a condiciones controladas, con el fin de determinar la influencia de un evento en particular.

Según Carrasco (2007) “Se aplica este nivel de investigación luego de identificar las características y las causas que la conciben como tal. Aquí se aplican diversas metodologías para mejorar la condición problemática” (p. 43).

El diseño de esta investigación fue experimental – pre experimental, debido a que en este caso se aplicó la variable independiente (Reconocimiento Biométrico por Huella Dactilar) para examinar las derivaciones que se tiene sobre la variable dependiente (Seguridad Lógica). Conforme a lo anterior, es pre experimental debido a que se limitó a observar en circunstancias naturales el efecto analizado sin intervención o modificación.

Según Carrasco (2007) “denomina diseños pre experimentales a aquellas investigaciones en que su grado de control es mínimo y no cumplen con los requisitos de un verdadero experimento” (p. 63).

3.1.1. Variables y operacionalización

Variable independiente: Reconocimiento Biométrico por Huella Dactilar

Según Serratosa (2012) “El reconocimiento biométrico se refiere al uso de diferentes características anatómicas (como huellas dactilares). Estas características se

denominan identificadores biométricos o rasgos biométricos y sirven para reconocer automáticamente a los individuos" (p.14).

Variable dependiente: Seguridad Lógica

Según Escrivá et al. (2013) "La seguridad lógica es el conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas. Así como a garantizar el acceso a la información únicamente por personas autorizadas" (p. 45).

En la Variable dependiente (Seguridad Lógica) se analizó tres dimensiones, divididas en 8 indicadores que dieron como resultado quince ítems.

Tabla 01: Operacionalización de la Variable Dependiente

Variable	Dimensión	Indicadores	Ítems
Dependiente: Seguridad Lógica	D.1. Control de Control	D.1.1. Eficiencia	1. Dificultad de acceso 2. Tiempo de acceso
		D.1.2. Seguridad de acceso	3. Autenticación 4. Autorización
		D.1.3. Gestión de credenciales	5. Olvido de credenciales 6. Cantidad de credenciales
	D.2. Ingeniería Social	D.2.1. Amenaza	7. Descuido del usuario 8. Espionaje corporativo
		D.2.2. Ataque	9. Manipulación
		D.2.3. Cooperación	10. Limitación 11. Cooperación del usuario
	D.3. Auditoria de Seguridad	D.3.1. Confiabilidad	12. Aseguramiento de identidad 13. Registro de actividad
		D.3.2. Accesibilidad	13. Ruptura de credenciales 14. Robo de credenciales

Fuente: Elaboración Propia

3.1.2. Población, muestra, muestreo, unicidad de análisis

La Población según Carrasco (2007) “Es el conjunto de todos los elementos (unidades de análisis) que pertenecen al ámbito espacial donde se desarrolla el trabajo de investigación” (p. 236).

En la presente investigación debido a ciertos factores de seguridad corporativa relacionados con la confidencialidad, disponibilidad e integridad de la información, asimismo, por factores socioeconómicos, se determinó una población conformada por el Equipo Servicios y Clientes Especiales, perteneciente a la Gerencia Comercial de SEDAPAL.

La muestra según Carrasco (2007),” Es una parte o fragmento representativo de la población, cuyas características esenciales son las de ser objetiva y reflejo fiel de ella, de tal manera que los resultados obtenidos en la muestra puedan generalizarse a todos los elementos que conforman dicha población” (p. 237).

En la presente investigación se determinó una muestra censal, para lo cual se seleccionó a los 52 trabajadores del Equipo Servicios y Clientes Especiales de la Gerencia Comercial, SEDAPAL, de acuerdo a su disponibilidad y en base a las características de evaluación pertinentes para la investigación.

3.2. Técnicas e instrumentos de recolección de datos

Según Carrasco (2007) “Las técnicas como herramientas procedimentales y estratégicas suponen un previo conocimiento en cuanto a su utilidad y aplicación, de tal manera que seleccionarlas y elegirlas resulta una tarea fácil para el investigador” (p. 274).

En la investigación se utilizó la técnica de la encuesta por ser de carácter masivo, expeditivo y módico, que permitió recoger información a través de un conjunto de preguntas, las cuales permitieron expresar como la Aplicación del Reconocimiento Biométrico influye en la Seguridad Lógica, asimismo, se registró con veracidad la situación proporcional al problema existente, debido a que la información que se recolectó y analizó fue suministrada por los mismos actores, lo cual permitió la validación de las hipótesis de la investigación.

Por otro lado, se utilizó la técnica del fichaje en el registro de la información relevante para la presente investigación.

3.3. Procedimientos

Según Carrasco (2007) “Los instrumentos de investigación cumplen roles muy importantes en la recogida de datos, y se aplican según la naturaleza, características del problema y la intencionalidad del objetivo de investigación” (p. 334).

Se aplicó el cuestionario como instrumento de medición para la variable dependiente, en la cual se administraron dos pruebas, la primera llamada pre prueba, para determinar la situación antes de aplicarle el estímulo, y la segunda para analizar el efecto posteriormente de la administración del estímulo. En cada pregunta se contó con 5 alternativas en base a la escala de Likert con la cual se pudo medir el grado de percepción, siendo las opciones de respuesta las siguientes:

Totalmente de acuerdo (5), de acuerdo (4), ni de acuerdo ni en desacuerdo (3), en desacuerdo (2), totalmente en desacuerdo (1).

El tiempo de aplicación del instrumento fue aproximadamente de 20 minutos. Por otro lado, cada una de las dos pruebas aplicadas consto de 15 preguntas conformadas en base al mismo contexto, derivadas de 3 dimensiones que fueron divididas en 8 indicadores que resultaron en 15 ítems con las cuales se determinaron las preguntas.

Tabla 02: Ficha Técnica de recolección de datos

Nombre del Instrumento	Cuestionario
Autores de la ficha	Jiménez Prada Ricardo Antonio Guerra Jiménez Gustavo Mauricio
Año de elaboración	2020
Dirigido	Colaboradores de SEDAPAL
Tiempo de Aplicación	25 minutos
Método de Aplicación	Encuesta
Periodo de Recolección	5 días calendario
Procedimiento de selección	Personal del área comercial
Método de Muestreo	Muestreo censal

Fuente: Elaboración Propia.

Confiabilidad del Instrumento

Carrasco (2007) “La confiabilidad es la cualidad o propiedad de un instrumento de medición, que le permite obtener los mismos resultados, al aplicarse una o más veces a la misma persona o grupos de personas en diferentes periodos de tiempo” (p. 339).

Tabla 03: Estadística de fiabilidad

Alfa de Cronbach	N° de elementos
93.3%	15

Fuente: SPSS

El Coeficiente Alfa obtenido α=93.3% lo cual permite decir que el cuestionario en su versión de 15 ítems tiene una fuerte confiabilidad o una alta consistencia interna entre los ítems.

3.4. Método de análisis de datos

Sabino (1992) afirma que las actividades de recolección de datos nos brindaran los alcances necesarios enfocados a explicar la problemática inicial. Por otro lado, estos datos no brindaran ninguna orientación a alcanzar algún resultado ejecutorio, no sin antes suministrarles un debido tratamiento organizativo, con el fin de poseer una información uniforme en conjunto. (p. 186)

Se utilizó la prueba de rangos con signo de Wilcoxon, la cual es empleada para comparar el rango medio de dos muestras relacionadas y comprobar si existen diferencias entre ellas, en la cual utiliza el nivel ordinal de la variable dependiente para establecer si los resultados obtenidos fueron al azar o no, es decir si para hallar el efecto que existe en la seguridad lógica por parte de la aplicación del Reconocimiento Biométrico por Huella Dactilar.

El correcto análisis de los datos se determinó de acuerdo a los valores obtenidos debido a la aplicación del cuestionario, instrumento seleccionado para la recolección de los datos, elaborado para la variable dependiente, la cual fue medida en dos

pruebas, la primera antes de la intervención del tratamiento y la segunda con la aplicación del estímulo.

Se elaboró una base de datos para ambas pruebas de la variable dependiente, con la finalidad de agilizar el análisis de los datos y garantizar su posterior interpretación.

Para el correcto análisis de la variable dependiente se empleó el sistema operativo Windows 8 Intel Core i5. Por otro lado, se utilizaron los programas Microsoft Office Excel 2016 para Windows y el programa estadístico SPSS statistics para el procesamiento de la información.

Para medir la variable dependiente, se recolectó información a partir de las siguientes dimensiones: Control de acceso, Ingeniería social y Auditoria de seguridad. La información obtenida se incorporó en el programa estadístico informático SPSS statistical Package for Social Sciences (SPSS), el cual fue una herramienta importante para la consolidación del presente trabajo de investigación.

Para el análisis de los datos se elaboró teniendo en cuenta los niveles de medición de la variable, los cuales permitieron describir y establecer las principales propiedades de la variable en las distintas pruebas tomadas individualmente.

3.5. Aspectos éticos

Dentro de los principios éticos de la empresa, se solicitó la autorización respectiva, la misma que fue correspondida de forma consiente, voluntaria y totalmente trasparente.

Los colaboradores fueron informados días previos de la aplicación de la encuesta a fin de obtener resultados objetivos acorde a la percepción personal de cada colaborador.

La encuesta se empleó con altos niveles de respeto, amabilidad y honestidad. No se manipularon los resultados del instrumento aplicado y se procedió con ética a pesar de que pudieron salir inválidos los resultados.

La presente investigación se elaboró respetando los derechos de autor de otros trabajos de investigación, ensayos, libros, revistas científicas y otras fuentes de información que fueron útiles para la consolidación del presente trabajo de investigación.

IV. RESULTADOS

4.1. Descripción y análisis estadístico

Para la variable dependiente “Seguridad Lógica” se analizaron dos pruebas, la primera antes de la aplicación del modelo de “Reconocimiento biométrico por Huella Dactilar” y la segunda posterior a la aplicación; cada prueba se ordena de acuerdo a 15 preguntas, agrupadas en 3 dimensiones y 8 indicadores. En la presente investigación se muestran las tablas y figuras procedentes de cada pregunta, donde se concibe los resultados obtenidos y las interpretaciones por parte de los autores.

4.1.1. Pre prueba de la variable dependiente: Seguridad Lógica

En la primera medición concedida como “Pre prueba”, se aplicó 15 preguntas derivadas de 3 dimensiones: Control de Acceso, Ingeniería social y Auditoria de Seguridad, las cuales se analizaron e interpretaron a través de tablas de frecuencia y figuras representadas en gráficos de barras.

Dimensión 1: Control de acceso

Tabla 04: Pre Prueba - No resulta tedioso a los usuarios ingresar las credenciales de acceso a los programas informáticos.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	16	30,8	30,8	30,8
En Desacuerdo	22	42,3	42,3	73,1
Ni de acuerdo ni en desacuerdo	10	19,2	19,2	92,3
De acuerdo	4	7,7	7,7	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

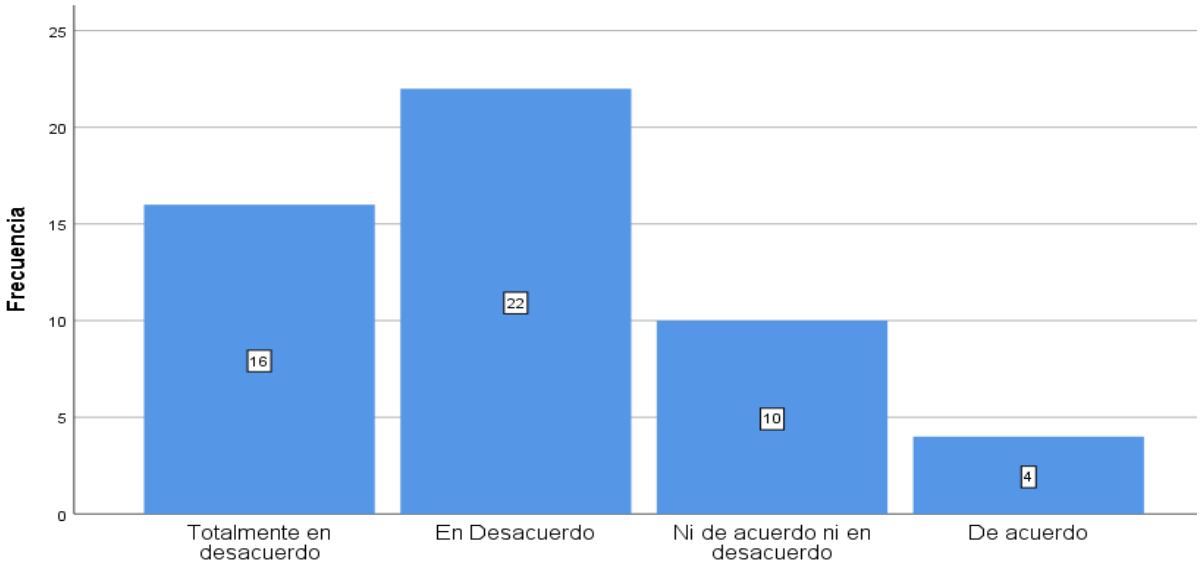


Figura 01: Pre Prueba - No resulta tedioso a los usuarios ingresar las credenciales de acceso a los programas informáticos.

Se observa que el 42.3% y 30.8 % de la población encuestada está en desacuerdo y totalmente en desacuerdo respectivamente en que no resulta tedioso a los usuarios ingresar las credenciales de acceso a los programas informáticos, mientras que el 7.7 % está de acuerdo en que no resulta tedioso.

En la figura 1 se puede tomar como referencia que 22 y 16 de 52 colaboradores están en desacuerdo y totalmente en desacuerdo respectivamente en que no resulta tedioso ingresar las credenciales de acceso a los programas informáticos.

Tabla 05: Pre Prueba - El tiempo para el proceso de autenticación es óptimo.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	20	38,5	38,5	38,5
En Desacuerdo	21	40,4	40,4	78,8
Ni de acuerdo ni en desacuerdo	11	21,2	21,2	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia

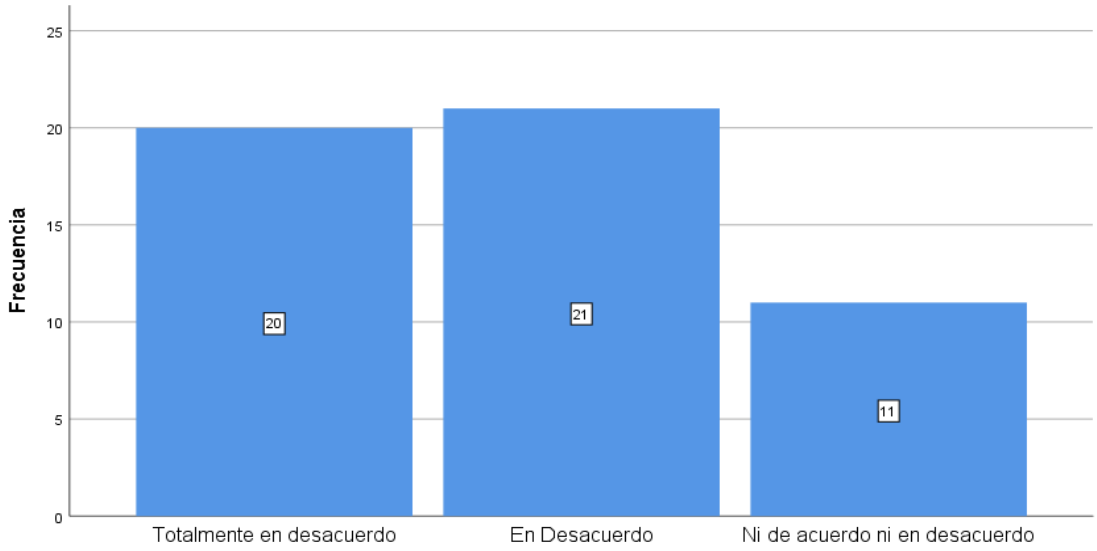


Figura 02. Pre Prueba - El tiempo para el proceso de autenticación es óptimo.

En la tabla 5 se puede apreciar que el 40.4% de la población encuestada está en desacuerdo en que el tiempo para el proceso de autenticación es óptimo, asimismo el 38.5 % está totalmente en desacuerdo de que el tiempo de autenticación es óptimo.

Se puede tomar como referencia en la figura 2, en que 21 y 20 de 52 colaboradores están en desacuerdo y totalmente en desacuerdo correspondientemente de que el tiempo para el proceso de autenticación es óptimo.

Tabla 06: Pre Prueba - La autenticación de usuarios a los programas informáticos es segura

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	17	32,7	32,7	32,7
En Desacuerdo	24	46,2	46,2	78,8
Ni de acuerdo ni en desacuerdo	9	17,3	17,3	96,2
De acuerdo	2	3,8	3,8	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

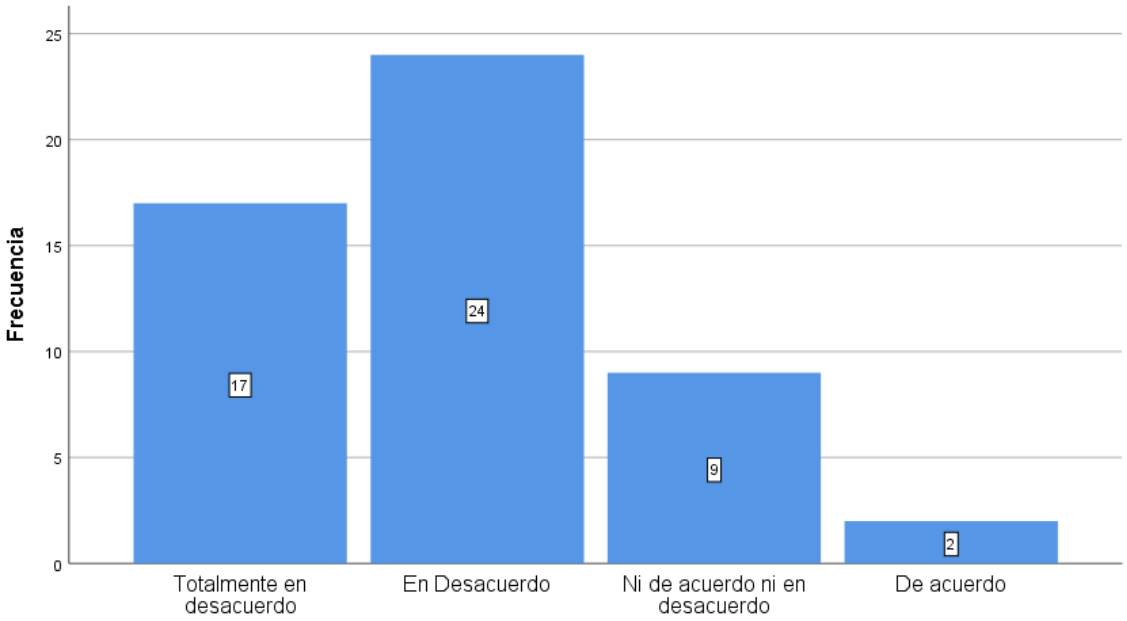


Figura 03. Pre Prueba - La autenticación de usuarios a los programas informáticos es segura.

En la tabla 6 se observa que el 46.2 % de la población encuestada está en desacuerdo con que la autenticación de usuarios a los programas informáticos es segura, mientras que 3.8 % están de acuerdo de que la autenticación de usuarios es segura.

Se referencia que 24 de 52 colaboradores están en desacuerdo de que la autenticación es segura.

Tabla 07: Pre Prueba - El proceso de autenticación permite el acceso a una cuenta solo a la persona autorizada.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	15	28,8	28,8	28,8
En Desacuerdo	23	44,2	44,2	73,1
Ni de acuerdo ni en desacuerdo	11	21,2	21,2	94,2
De acuerdo	3	5,8	5,8	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

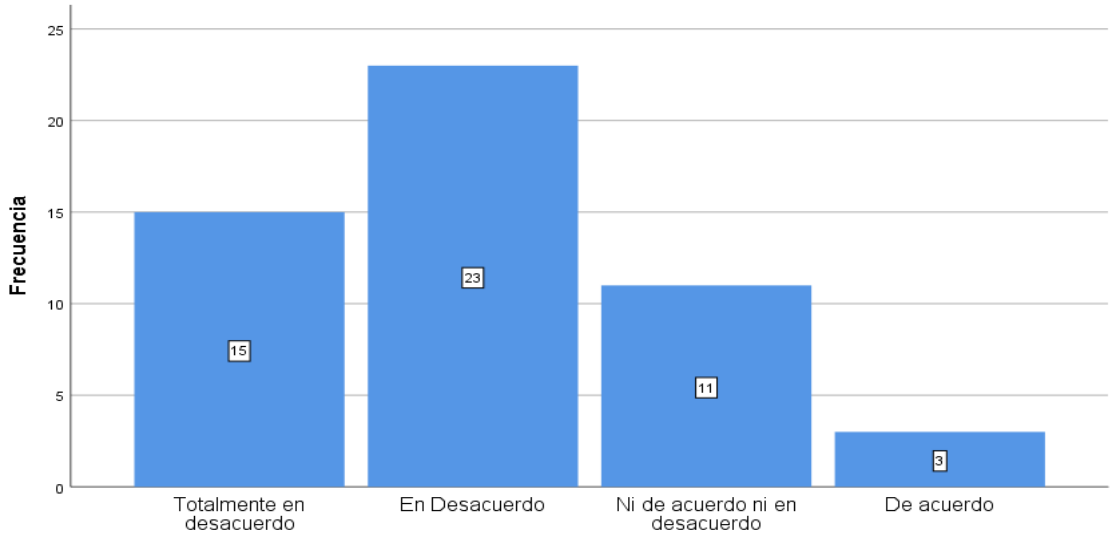


Figura 04. Pre Prueba - El proceso de autenticación permite el acceso a una cuenta solo a la persona autorizada.

Se puede observar que el 44.2 % el cual corresponde a 23 de 52 colaboradores de la población encuestada está en desacuerdo con que el proceso de autenticación permite el acceso a una cuenta solo a la persona autorizada, mientras que el 5.8% que representa a 3 de 52 colaboradores encuestados están de acuerdo de que el acceso es plenamente de la persona autorizada.

Tabla 08: Pre Prueba - Las credenciales de acceso de los usuarios no tienden a ser olvidadas.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	13	25,0	25,0	25,0
En Desacuerdo	23	44,2	44,2	69,2
Ni de acuerdo ni en desacuerdo	12	23,1	23,1	92,3
De acuerdo	3	5,8	5,8	98,1
Totalmente de acuerdo	1	1,9	1,9	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

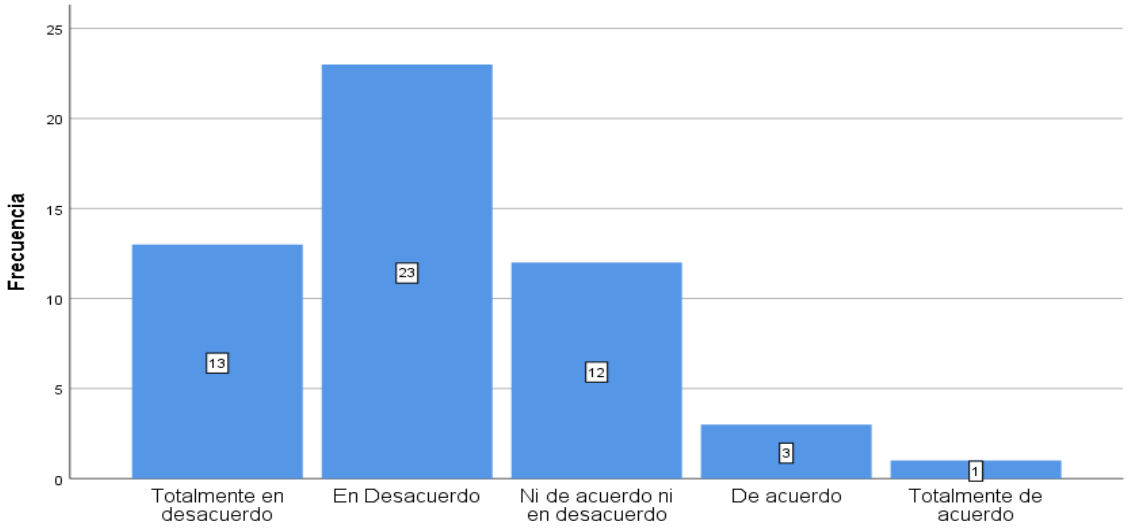


Figura 05. Pre Prueba - Las credenciales de acceso de los usuarios no tienden a ser olvidadas.

Se puede observar que el 44.2 % de la población encuestada está en desacuerdo con que las credenciales acceso de los usuarios no tienden a ser olvidadas, mientras que 5.8 % están de acuerdo de que las credenciales no tienden a ser olvidadas.

Se toma como referencia en la figura 5, en que 23 de 52 colaboradores están en desacuerdo en que las credenciales de acceso de los usuarios no tienden a ser olvidadas.

Tabla 09: Pre Prueba - La cantidad de credenciales asignadas a los usuarios para acceder a los programas informáticos es adecuado

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	17	32,7	32,7	32,7
En Desacuerdo	23	44,2	44,2	76,9
Ni de acuerdo ni en desacuerdo	8	15,4	15,4	92,3
De acuerdo	3	5,8	5,8	98,1
Totalmente de acuerdo	1	1,9	1,9	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

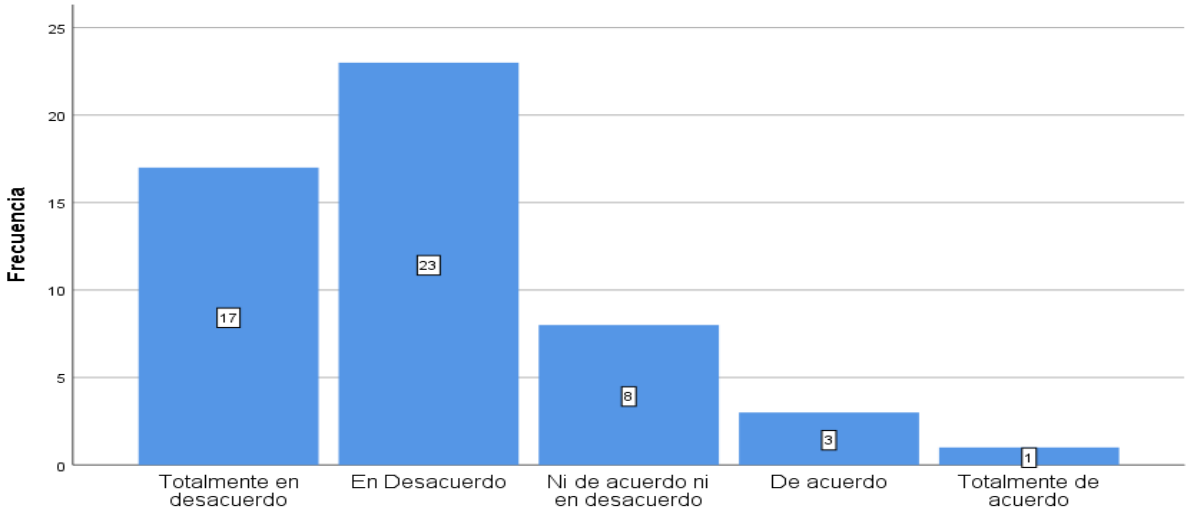


Figura 06. Pre Prueba - La cantidad de credenciales asignadas a los usuarios para acceder a los programas informáticos es adecuado.

Se puede examinar que el 42.2 % que referencia a 23 de 52 colaboradores de la población encuestada está en desacuerdo con que la cantidad de credenciales asignadas a los usuarios para acceder a los programas informáticos es adecuada, mientras que el 5.8 % está de acuerdo en que la cantidad de credenciales asignadas es adecuada.

Dimensión 2: Ingeniería Social

Tabla 10: Pre Prueba - El descuido del usuario no representa una amenaza para el proceso de autenticación.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	14	26,9	26,9	26,9
En Desacuerdo	22	42,3	42,3	69,2
Ni de acuerdo ni en desacuerdo	12	23,1	23,1	92,3
De acuerdo	3	5,8	5,8	98,1
Totalmente de acuerdo	1	1,9	1,9	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

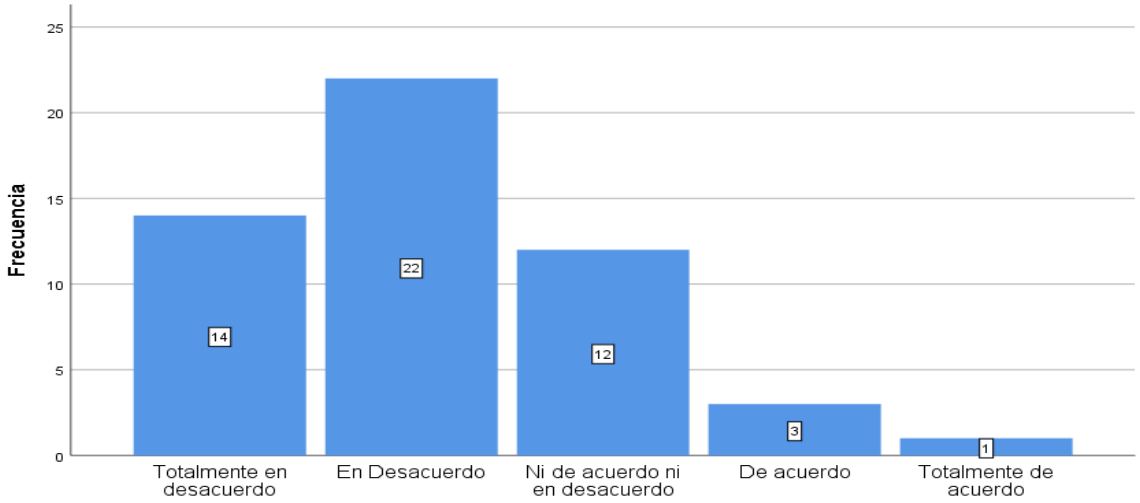


Figura 07. Pre Prueba - El descuido del usuario no representa una amenaza para el proceso de autenticación.

Se puede reconocer que el 42.3 % de la población encuestada está en desacuerdo mientras que 5.8% está de acuerdo orientado a que el descuido no representa una amenaza para la autenticación.

Se señala como referencia que 22 de 52 colaboradores están en desacuerdo de que el descuido por parte del usuario no representa una amenaza para el proceso de autenticación.

Tabla 11: Pre Prueba - El espionaje corporativo no es una amenaza difícil de detectar en el proceso de autenticación de usuarios.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	16	30,8	30,8	30,8
En Desacuerdo	21	40,4	40,4	71,2
Ni de acuerdo ni en desacuerdo	11	21,2	21,2	92,3
De acuerdo	3	5,8	5,8	98,1
Totalmente de acuerdo	1	1,9	1,9	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

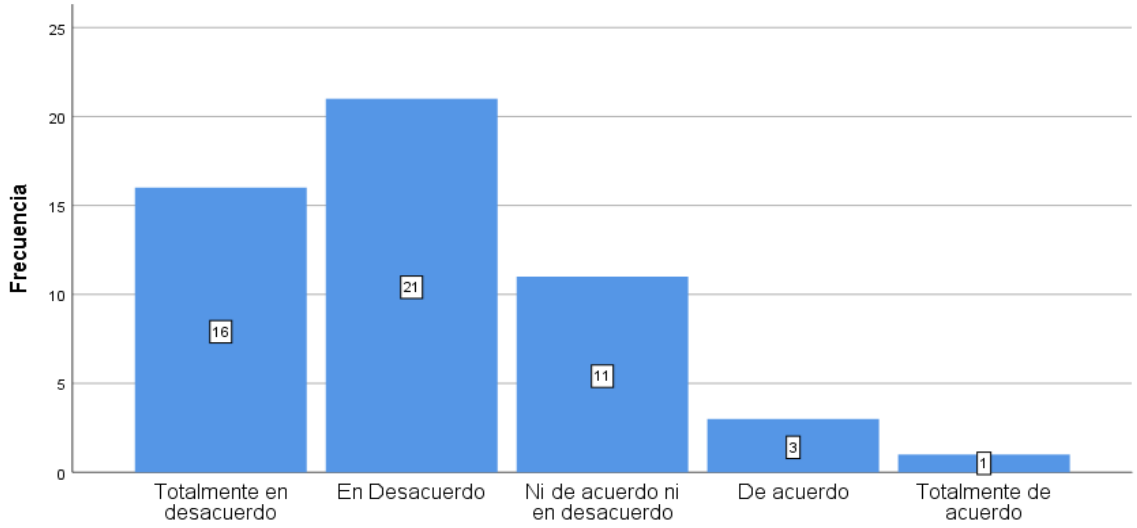


Figura 08. Pre Prueba - El espionaje corporativo no es una amenaza difícil de detectar en el proceso de autenticación de usuarios.

Se puede examinar que el 21.2 % de la población encuestada opina que está en desacuerdo, mientras que el 5.8 % está de acuerdo de que el espionaje corporativo no es una amenaza dificultosa de descubrir en el proceso de autenticación.

Se indica como referencia que 21 de 52 colaboradores manifiestan que están en desacuerdo de que el espionaje corporativo no representa una amenaza difícil de detectar en el proceso de autenticación.

Tabla 12: Pre Prueba - El proceso de autenticación es propenso a un ataque por manipulación de personas.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	18	34,6	34,6	34,6
En Desacuerdo	19	36,5	36,5	71,2
Ni de acuerdo ni en desacuerdo	13	25,0	25,0	96,2
De acuerdo	2	3,8	3,8	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

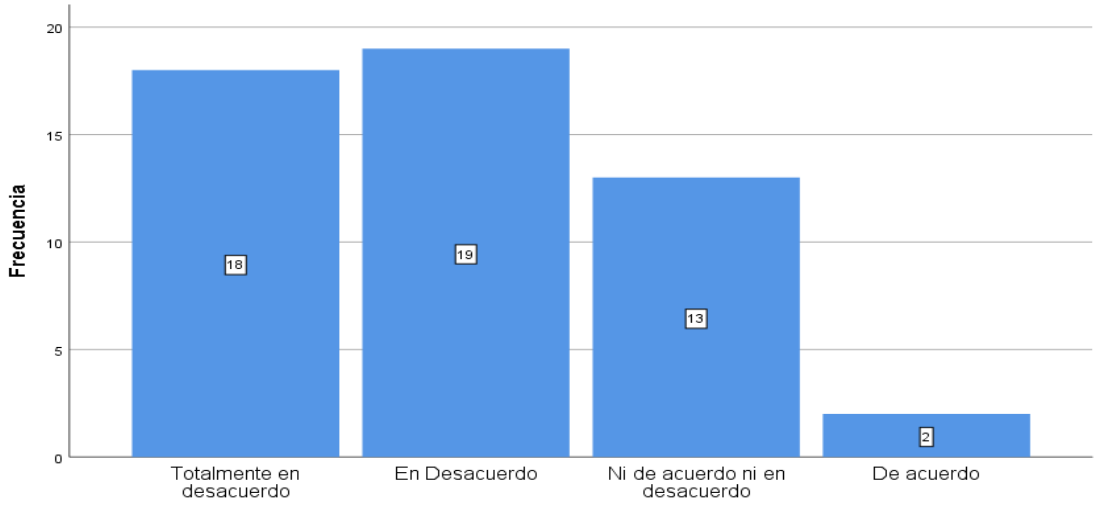


Figura 09. Pre Prueba - El proceso de autenticación es propenso a un ataque por manipulación de personas.

Se observa que el 36.5 % de la población encuestada menciona que está en desacuerdo, mientras que el 3.8 % está de acuerdo respectivamente, enfocado a que la autenticación es propensa a un ataque de manipulación a personas, asimismo, se señala como referencia que 19 de 52 colaboradores manifiestan que están en desacuerdo que el proceso de autenticación es propenso a un ataque por manipulación de personas.

Tabla 13: Pre Prueba - El proceso de autenticación limita a los usuarios compartir sus credenciales con otras personas.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	16	30,8	30,8	30,8
En Desacuerdo	20	38,5	38,5	69,2
Ni de acuerdo ni en desacuerdo	12	23,1	23,1	92,3
De acuerdo	3	5,8	5,8	98,1
Totalmente de acuerdo	1	1,9	1,9	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

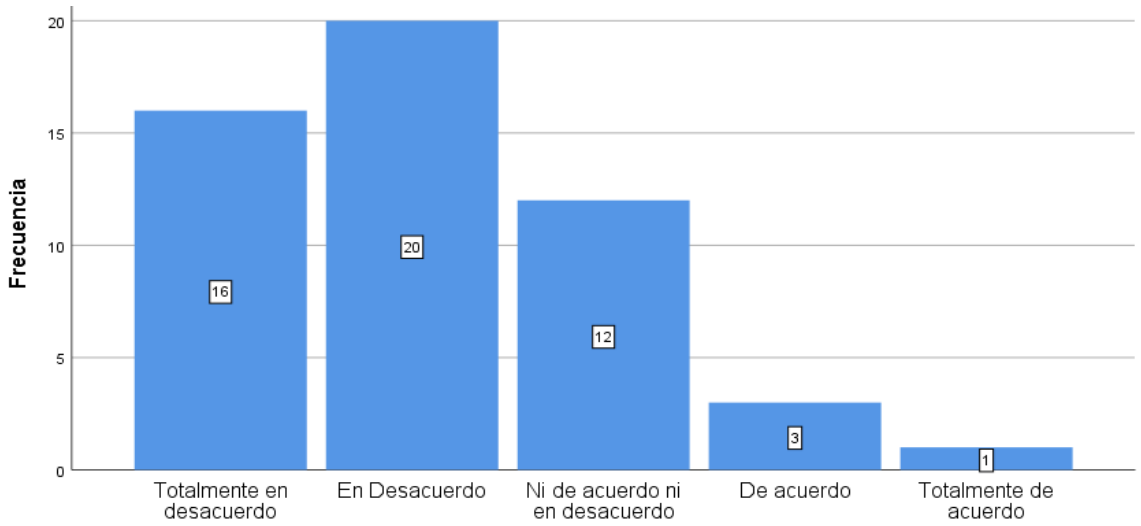


Figura 10. Pre Prueba - El proceso de autenticación limita a los usuarios compartir sus credenciales con otras personas.

Se aprecia que el 39.5 % de la población encuestada menciona que está en desacuerdo, mientras el 5.8 % está de acuerdo a que el proceso de autenticación limita a los usuarios compartir sus credenciales con otras personas.

Se señala como referencia que 20 de 52 colaboradores revelan que están en desacuerdo de que el proceso de autenticación los limita compartir sus credenciales con otras personas.

Tabla 14: Pre Prueba - La cooperación consiente de un usuario en un ataque informático que no afecta el proceso de autenticación.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	16	30,8	30,8	30,8
En Desacuerdo	19	36,5	36,5	67,3
Ni de acuerdo ni en desacuerdo	11	21,2	21,2	88,5
De acuerdo	4	7,7	7,7	96,2
Totalmente de acuerdo	2	3,8	3,8	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

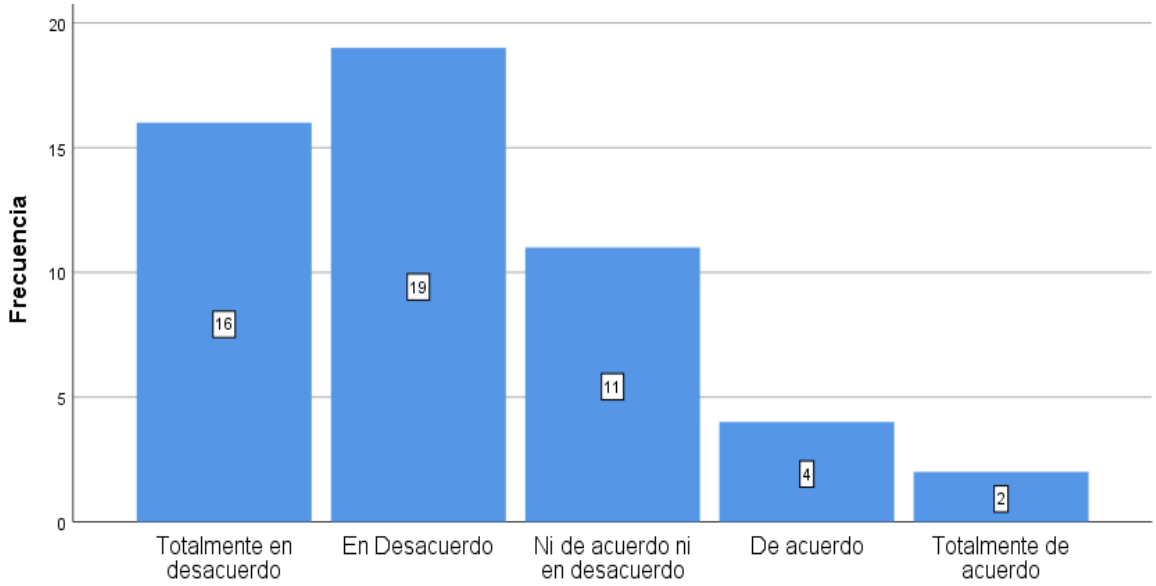


Figura 11. Pre Prueba - La cooperación consiente de un usuario en un ataque informático que no afecta el proceso de autenticación.

Se evalúa que el 36.5 % que corresponde a 19 de 52 colaboradores de la población encuestada alude que está en desacuerdo, mientras que el 7.7 % está de acuerdo respecto a que la cooperación del usuario en forma consiente dentro de un ataque informático no afecta el proceso de autenticación.

Dimensión 3: Auditoria de Seguridad

Tabla 15: Pre Prueba - El proceso de autenticación permite asegurar la identidad veraz de una persona asociado a la cuenta con la que accedió.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	16	30,8	30,8	30,8
En Desacuerdo	21	40,4	40,4	71,2
Ni de acuerdo ni en desacuerdo	11	21,2	21,2	92,3
De acuerdo	4	7,7	7,7	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

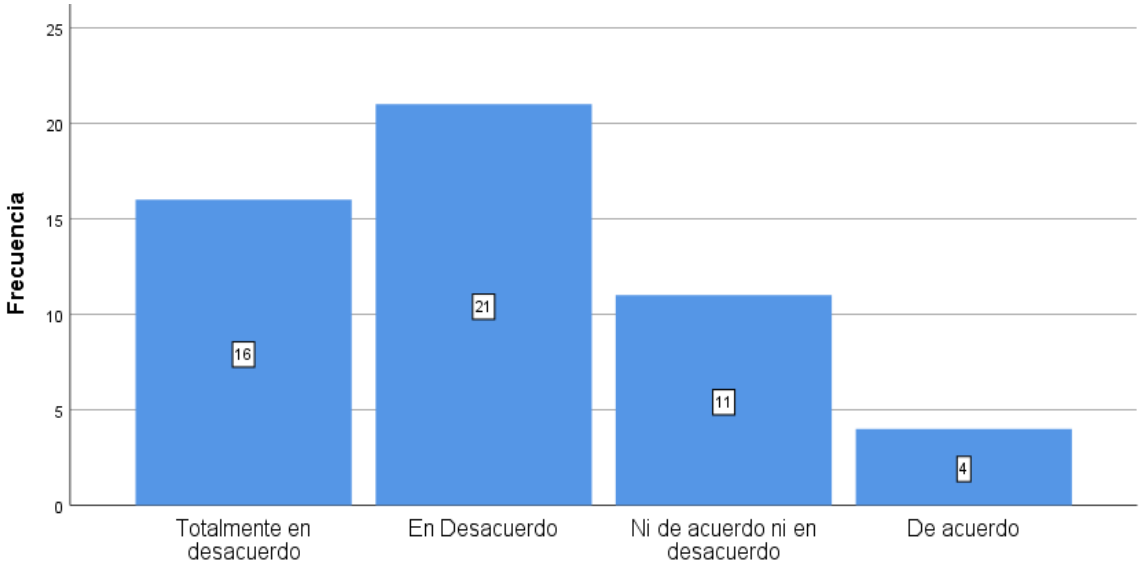


Figura 12. Pre Prueba - El proceso de autenticación permite asegurar la identidad veraz de una persona asociado a la cuenta con la que accedió.

Se aprecia que el 40.4 % que referencia a 21 de 52 colaboradores de la población encuestada está en desacuerdo, mientras que el 7.7 % está totalmente de acuerdo y de acuerdo, respecto a que el proceso de autenticación permite asegurar de forma veraz la identidad de una persona asociada a la cuenta con la que accedió.

Tabla 16: Pre Prueba El proceso de autenticación permite llevar un registro de actividad confiable de los usuarios dentro del sistema.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	16	30,8	30,8	30,8
En Desacuerdo	18	34,6	34,6	65,4
Ni de acuerdo ni en desacuerdo	15	28,8	28,8	94,2
De acuerdo	2	3,8	3,8	98,1
Totalmente de acuerdo	1	1,9	1,9	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

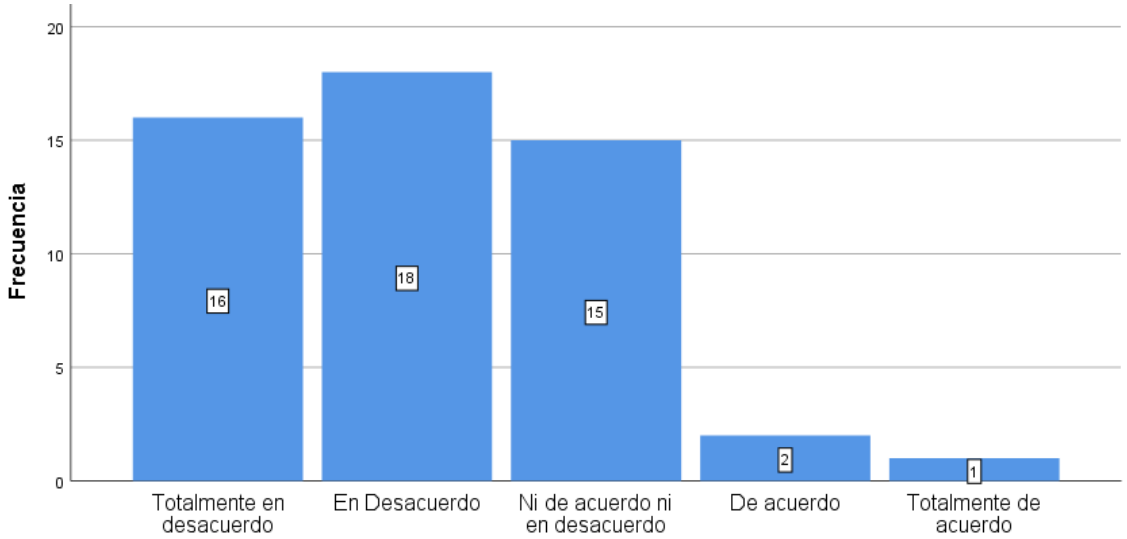


Figura 13. Pre Prueba El proceso de autenticación permite llevar un registro de actividad confiable de los usuarios dentro del sistema.

Se observa que el 34.6 % de la población encuestada revela que está en desacuerdo, mientras que el 3.8 % está de acuerdo, respecto a que el proceso de autenticación permite llevar un registro de actividad confiable de los usuarios dentro del sistema.

Se precisa como referencia que 18 de 52 colaboradores están en desacuerdo de que la autenticación permite asegurar de forma veraz la identidad de una persona de acuerdo con la cuenta asociada con la que accedió.

Tabla 17: Pre Prueba - El proceso de autenticación de usuarios permite minimizar la ruptura de credenciales de acceso.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	19	36,5	36,5	36,5
En Desacuerdo	24	46,2	46,2	82,7
Ni de acuerdo ni en desacuerdo	7	13,5	13,5	96,2
De acuerdo	2	3,8	3,8	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

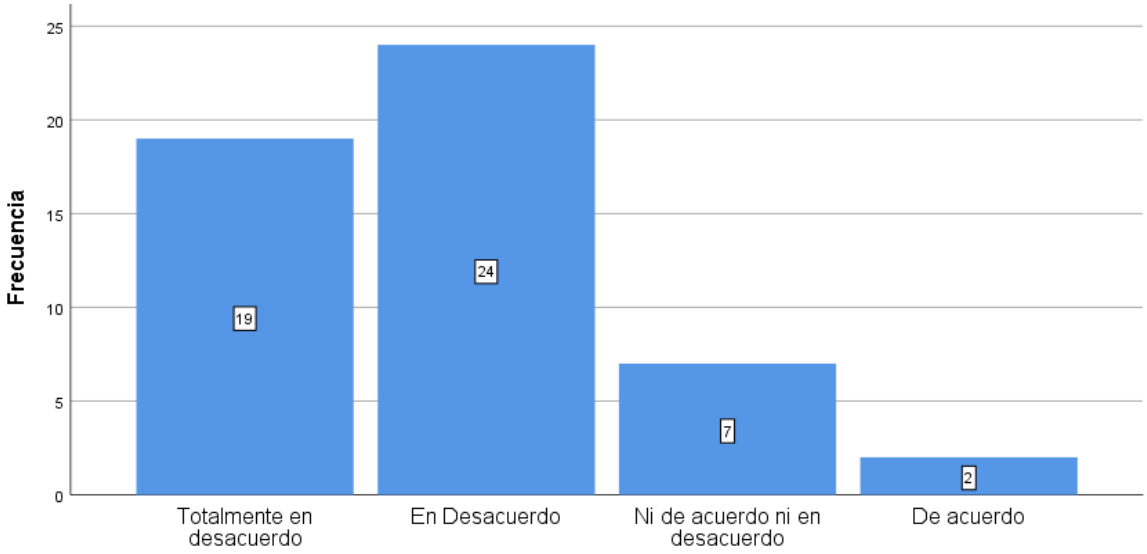


Figura 14. Pre Prueba - El proceso de autenticación de usuarios permite minimizar la ruptura de credenciales de acceso.

Se observa que el 46.2 % de la población encuestada revela que está en desacuerdo, mientras que el 3.8 % está de acuerdo correspondientemente, en relación a que el proceso de autenticación de usuarios permite minimizar la ruptura de credenciales de acceso.

Se precisa como referencia que 24 de 52 colaboradores están en desacuerdo respectivamente de que el proceso de autenticación permite minimizar la ruptura de credenciales de acceso.

Tabla 18: Pre Prueba - La autenticación de usuarios no está sujeto al robo de credenciales.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	20	38,5	38,5	38,5
En Desacuerdo	17	32,7	32,7	71,2
Ni de acuerdo ni en desacuerdo	9	17,3	17,3	88,5
De acuerdo	6	11,5	11,5	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

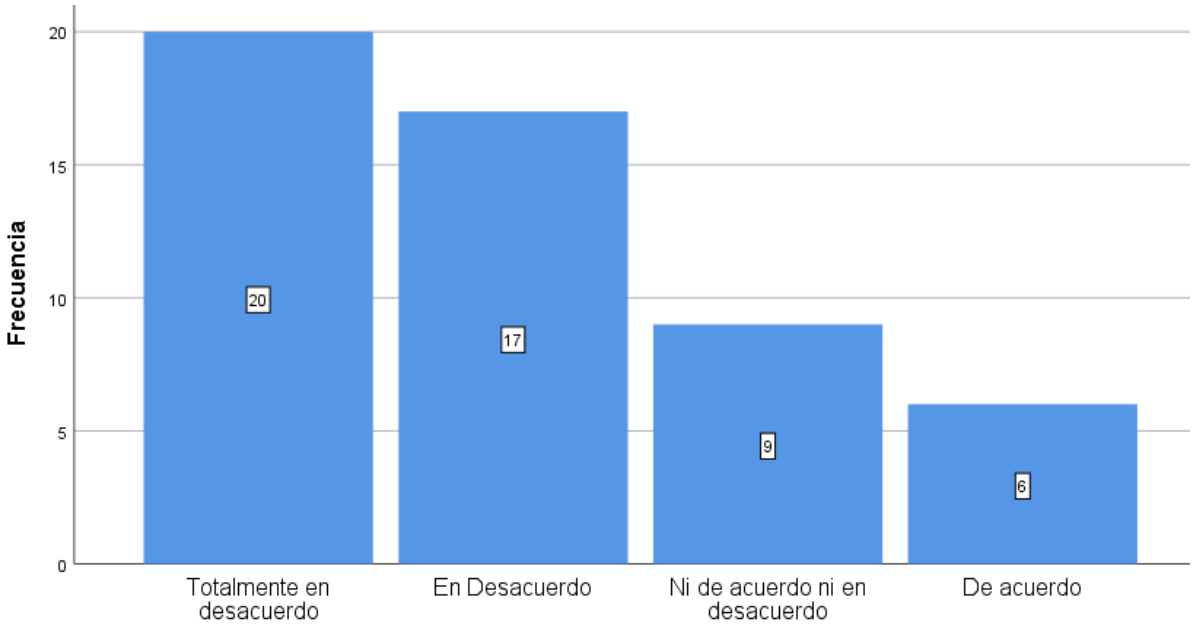


Figura 15. Pre Prueba - La autenticación de usuarios no está sujeto al robo de credenciales.

Se observa que el 32.7 % de la población encuestada revela que está en desacuerdo y totalmente en desacuerdo, mientras que el 11.5 % está de acuerdo orientado a que la autenticación de usuarios no está sujeto al robo de credenciales.

Se señala como referencia que 17 y 20 de 52 colaboradores están en desacuerdo y totalmente en desacuerdo respectivamente de que la autenticación de usuarios no está sujeto al robo de credenciales.

4.1.2. Post prueba de la variable dependiente: Seguridad Lógica

En la segunda medición definida como “Post prueba”, se empleó 15 preguntas, totalmente iguales a las que se aplicaron en la “Pre prueba”, procedentes de las mismas dimensiones, las cuales son: Control de Acceso, Ingeniería social y Auditoria de seguridad, con el fin de estudiar y explicar por medio de tablas de frecuencia y figuras representados en gráficos de barras, asociadas a los datos obtenidos, las diferencias después de aplicar el Reconocimiento Biométrico por Huella Dactilar.

Dimensión 1: Control de acceso

Tabla 19: Post Prueba - No resulta tedioso a los usuarios ingresar las credenciales de acceso a los programas informáticos.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	2	3,8	3,8	3,8
En Desacuerdo	7	13,5	13,5	17,3
Ni de acuerdo ni en desacuerdo	14	26,9	26,9	44,2
De acuerdo	13	25,0	25,0	69,2
Totalmente de acuerdo	16	30,8	30,8	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

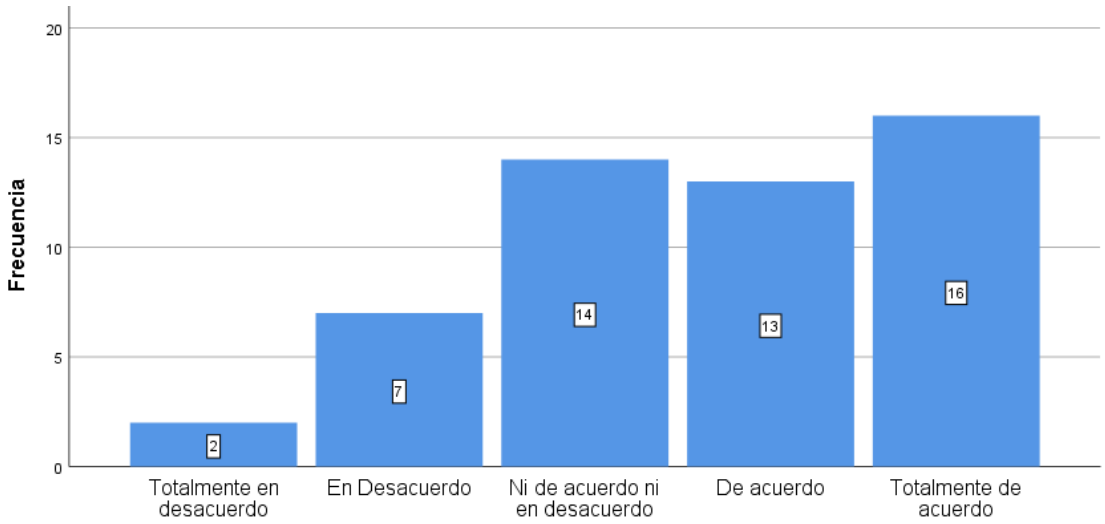


Figura 16. Post Prueba - No resulta tedioso a los usuarios ingresar las credenciales de acceso a los programas informáticos.

Se observa que el 13.5 % y 3.8 % de la población encuestada está en desacuerdo y totalmente en desacuerdo correspondientemente con que no resulta tedioso a los usuarios ingresar las credenciales de acceso a los programas informáticos, mientras que el 30.8 % y 25 % está totalmente de acuerdo y de acuerdo respectivamente de que no resulta tedioso.

En la figura se puede tomar como referencia que 13 y 16 de 52 colaboradores están de acuerdo y totalmente de acuerdo respectivamente de que no resulta tedioso ingresar las credenciales de acceso a los programas informáticos

Tabla 20: Post Prueba - El tiempo para el proceso de autenticación es óptimo.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	4	7,7	7,7	7,7
En Desacuerdo	7	13,5	13,5	21,2
Ni de acuerdo ni en desacuerdo	12	23,1	23,1	44,2
De acuerdo	13	25,0	25,0	69,2
Totalmente de acuerdo	16	30,8	30,8	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

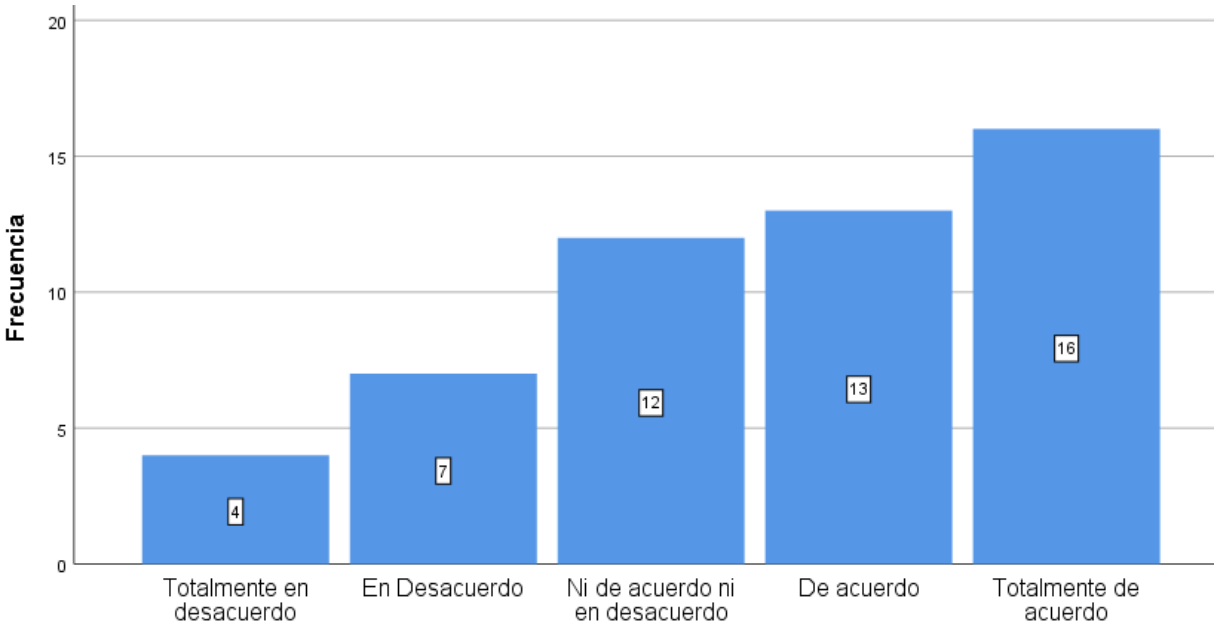


Figura 17. Post Prueba - El tiempo para el proceso de autenticación es óptimo.

En la tabla 20 se puede apreciar que el 25.0% de la población encuestada está de acuerdo con que el tiempo para el proceso de autenticación es óptimo, mientras que el 13.5 % está en desacuerdo de que el tiempo de autenticación es óptimo.

Se puede tomar como referencia que 13 y 16 de 52 colaboradores están de acuerdo y totalmente de acuerdo correspondientemente de que el tiempo para el proceso de autenticación es óptimo.

Tabla 21; Post Prueba - La autenticación de usuarios a los programas informáticos es segura.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	3	5,8	5,8	5,8
En Desacuerdo	12	23,1	23,1	28,8
Ni de acuerdo ni en desacuerdo	11	21,2	21,2	50,0
De acuerdo	16	30,8	30,8	80,8
Totalmente de acuerdo	10	19,2	19,2	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

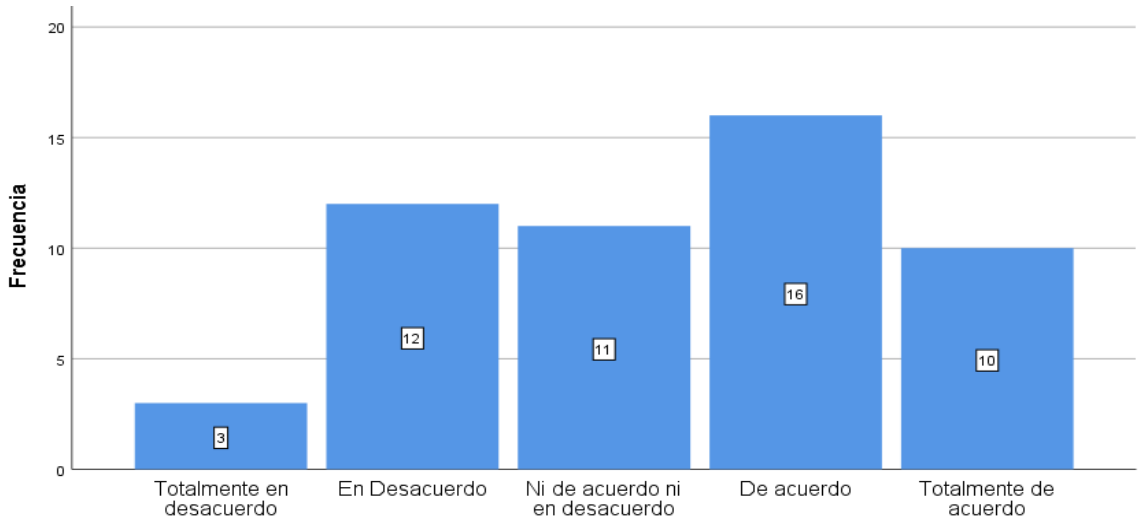


Figura 18. Post Prueba - La autenticación de usuarios a los programas informáticos es segura.

En la tabla se observa que el 23.1 % de la población encuestada está en desacuerdo con que la autenticación de usuarios a los programas informáticos es segura, mientras que 30.8 % están de acuerdo de que la autenticación de usuarios es segura.

Se referencia que 16 de 52 colaboradores están de acuerdo de que la autenticación es segura.

Tabla 22: Post Prueba - El proceso de autenticación permite el acceso a una cuenta solo a la persona autorizada.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	5	9,6	9,6	9,6
En Desacuerdo	8	15,4	15,4	25,0
Ni de acuerdo ni en desacuerdo	10	19,2	19,2	44,2
De acuerdo	16	30,8	30,8	75,0
Totalmente de acuerdo	13	25,0	25,0	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

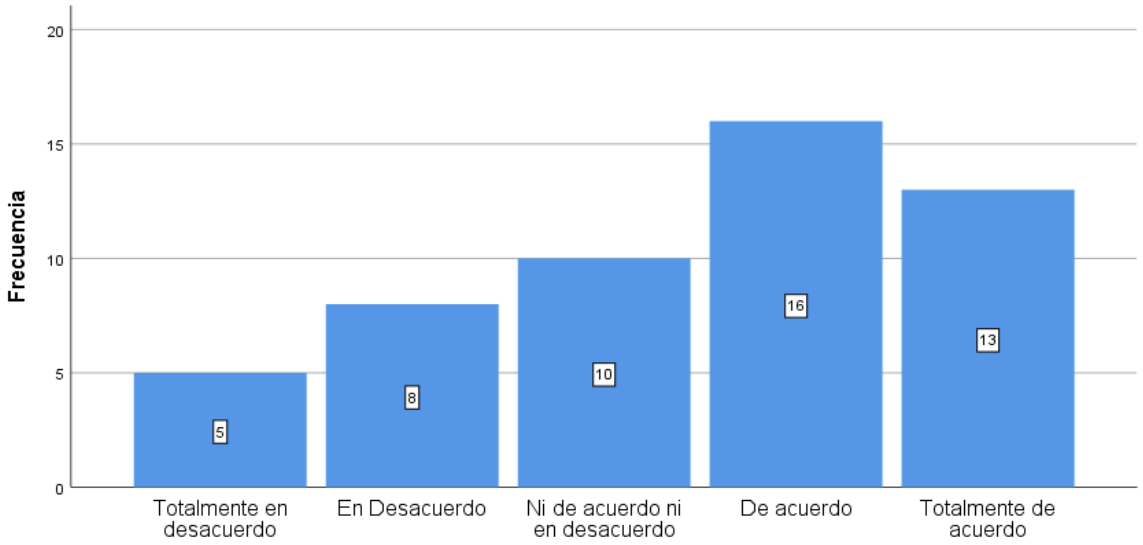


Figura 19. Post Prueba - El proceso de autenticación permite el acceso a una cuenta solo a la persona autorizada.

Se puede observar que el 30.8 % el cual corresponde a 16 de 52 colaboradores de la población encuestada está de acuerdo con que el proceso de autenticación permite el acceso a una cuenta solo a la persona autorizada, mientras que el 15.4 % que representa a 8 de 52 colaboradores encuestados están en desacuerdo de que el acceso es plenamente de la persona autorizada.

Tabla 23: Post Prueba - Las credenciales de acceso de los usuarios no tienden a ser olvidadas

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	3	5,8	5,8	5,8
En Desacuerdo	8	15,4	15,4	21,2
Ni de acuerdo ni en desacuerdo	9	17,3	17,3	38,5
De acuerdo	19	36,5	36,5	75,0
Totalmente de acuerdo	13	25,0	25,0	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

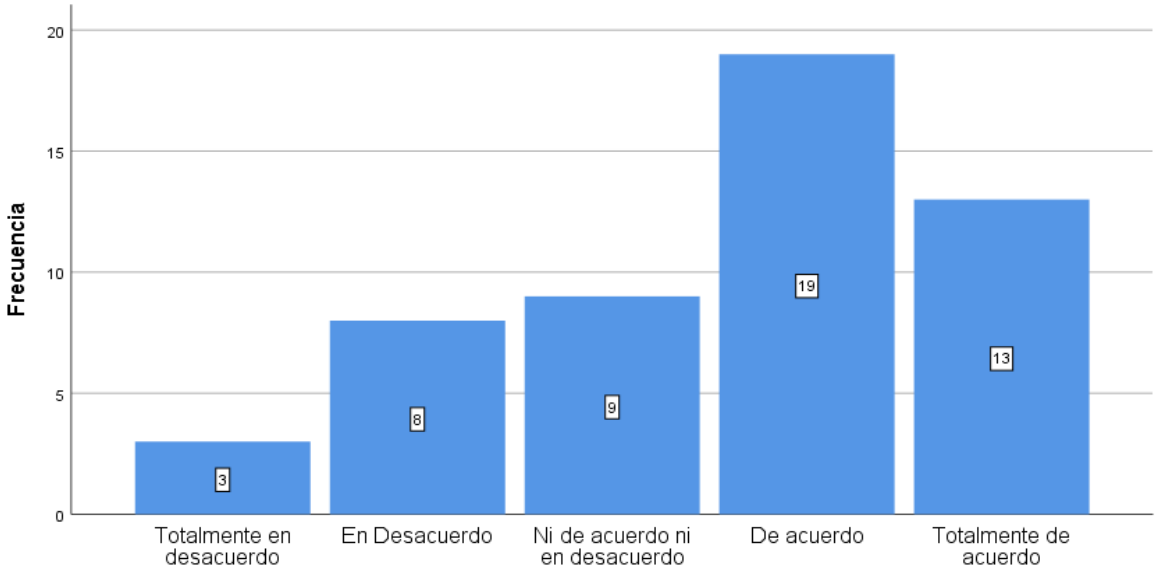


Figura 20. Post Prueba - Las credenciales de acceso de los usuarios no tienden a ser olvidadas.

Se puede observar que el 15.4 % de la población encuestada está en desacuerdo con que las credenciales acceso de los usuarios no tienden a ser olvidadas, mientras que 36.5 % están de acuerdo de que las credenciales no tienden a ser olvidadas.

Se toma como referencia que 19 de 52 colaboradores están de acuerdo de que las credenciales de acceso de los usuarios no tienden a ser olvidadas.

Tabla 24: Post Prueba - La cantidad de credenciales asignadas a los usuarios para acceder a los programas informáticos es adecuado.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	5	9,6	9,6	9,6
En Desacuerdo	4	7,7	7,7	17,3
Ni de acuerdo ni en desacuerdo	4	7,7	7,7	25,0
De acuerdo	23	44,2	44,2	69,2
Totalmente de acuerdo	16	30,8	30,8	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

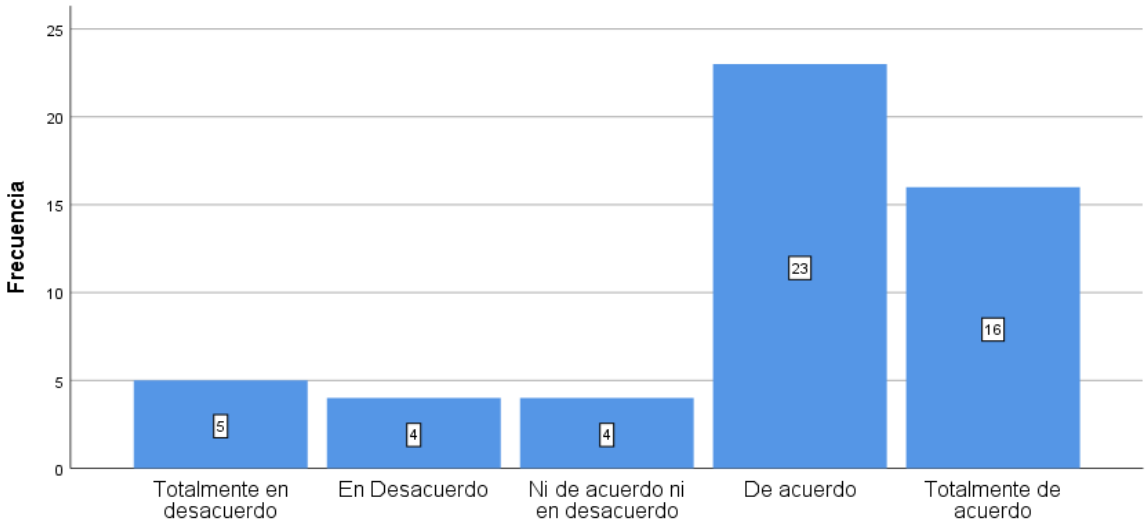


Figura 21. Post Prueba - La cantidad de credenciales asignadas a los usuarios para acceder a los programas informáticos es adecuado.

Se puede examinar que el 44.2 % que referencia a 23 de 52 colaboradores de la población encuestada está de acuerdo con que la cantidad de credenciales asignadas a los usuarios para acceder a los programas informáticos es adecuada, mientras que el 7.7 % está en desacuerdo de que la cantidad de credenciales asignadas es adecuada.

Dimensión 2: Ingeniería Social

Tabla 25: Post Prueba - El descuido del usuario no representa una amenaza para el proceso de autenticación

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	4	7,7	7,7	7,7
En Desacuerdo	9	17,3	17,3	25,0
Ni de acuerdo ni en desacuerdo	13	25,0	25,0	50,0
De acuerdo	12	23,1	23,1	73,1
Totalmente de acuerdo	14	26,9	26,9	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

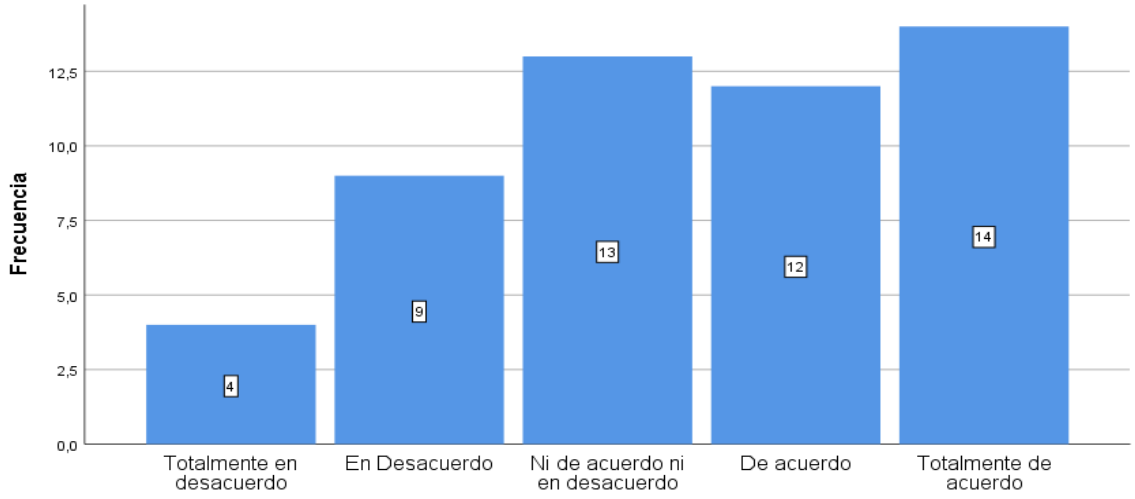


Figura 22. Post Prueba - El descuido del usuario no representa una amenaza para el proceso de autenticación.

Se puede reconocer que el 23.1 % de la población encuestada está de acuerdo mientras que 17.3 % está en desacuerdo orientado a que el descuido no representa una amenaza para la autenticación.

Se señala como referencia que 12 de 52 colaboradores están de acuerdo de que el descuido por parte del usuario no representa una amenaza para el proceso de autenticación.

Tabla 26: Post Prueba - El espionaje corporativo no es una amenaza difícil de detectar en el proceso de autenticación de usuarios.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	7	13,5	13,5	13,5
En Desacuerdo	10	19,2	19,2	32,7
Ni de acuerdo ni en desacuerdo	14	26,9	26,9	59,6
De acuerdo	13	25,0	25,0	84,6
Totalmente de acuerdo	8	15,4	15,4	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

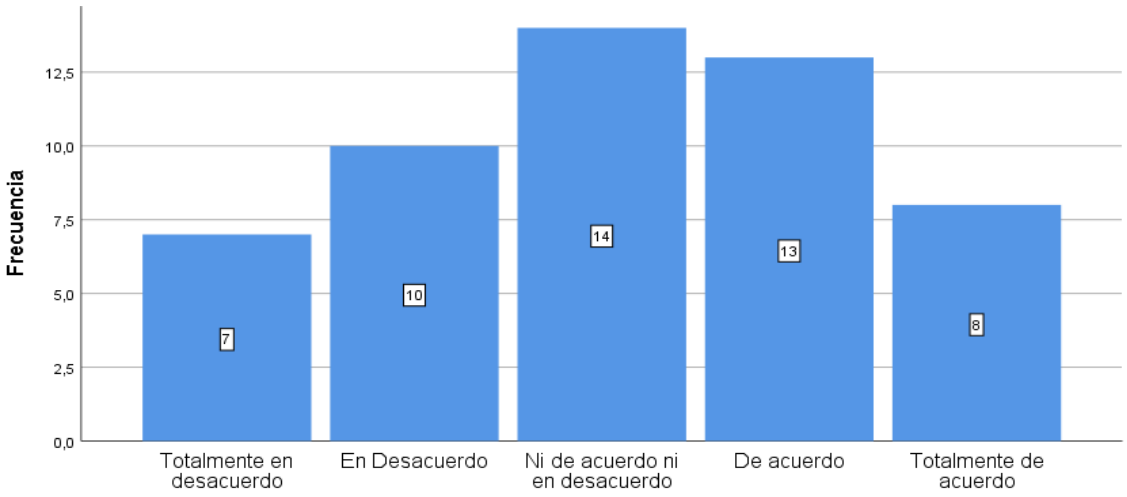


Figura 23. Post Prueba - El espionaje corporativo no es una amenaza difícil de detectar en el proceso de autenticación de usuarios.

Se puede examinar que el 19.2 % de la población encuestada opina que está en desacuerdo, mientras que el 25.0 % está de acuerdo de que el espionaje corporativo no es una amenaza dificultosa de descubrir en el proceso de autenticación.

Se indica como referencia que 13 de 52 colaboradores manifiestan que están de acuerdo de que el espionaje corporativo no representa una amenaza difícil de detectar en el proceso de autenticación.

Tabla 27: Post Prueba - El proceso de autenticación es propenso a un ataque por manipulación de personas.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	4	7,7	7,7	7,7
En Desacuerdo	10	19,2	19,2	26,9
Ni de acuerdo ni en desacuerdo	10	19,2	19,2	46,2
De acuerdo	16	30,8	30,8	76,9
Totalmente de acuerdo	12	23,1	23,1	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

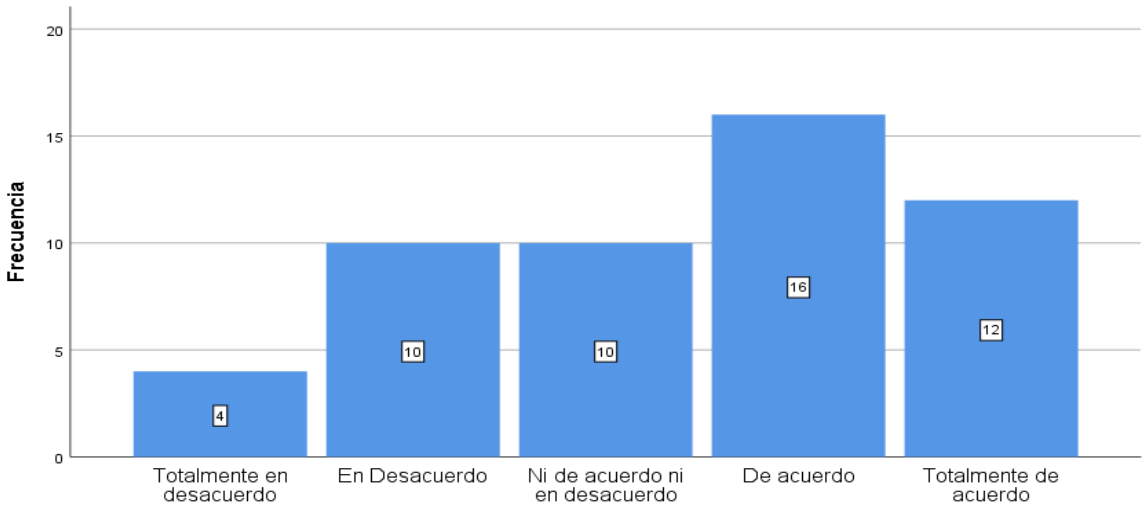


Figura 24. Post Prueba - El proceso de autenticación es propenso a un ataque por manipulación de personas.

Se observa que el 30.8 % de la población encuestada menciona que está de acuerdo, mientras que el 19.2 % está en desacuerdo respectivamente, enfocado a que la autenticación es propensa a un ataque de manipulación a personas.

Se señala como referencia que 16 de 52 colaboradores manifiestan que están de acuerdo que el proceso de autenticación es propenso a un ataque por manipulación de personas.

Tabla 28: Post Prueba - El proceso de autenticación limita a los usuarios compartir sus credenciales con otras personas.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	3	5,8	5,8	5,8
En Desacuerdo	5	9,6	9,6	15,4
Ni de acuerdo ni en desacuerdo	12	23,1	23,1	38,5
De acuerdo	20	38,5	38,5	76,9
Totalmente de acuerdo	12	23,1	23,1	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

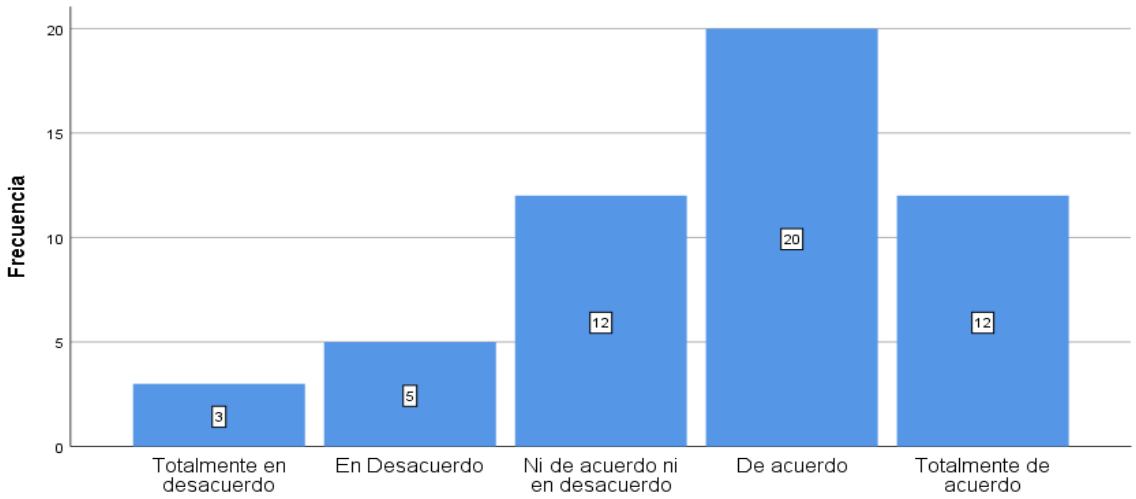


Figura 25. Post Prueba - El proceso de autenticación limita a los usuarios compartir sus credenciales con otras personas.

Se aprecia que el 38.5 % de la población encuestada menciona que está de acuerdo, mientras el 9.6 % está en desacuerdo a que el proceso de autenticación limita a los usuarios compartir sus credenciales con otras personas.

Se señala como referencia que 20 de 52 colaboradores revelan que están de acuerdo de que el proceso de autenticación los limita a compartir sus credenciales con otras personas.

Tabla 29: Post Prueba - La cooperación consiente de un usuario en un ataque informático que no afecta el proceso de autenticación.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	4	7,7	7,7	7,7
En Desacuerdo	5	9,6	9,6	17,3
Ni de acuerdo ni en desacuerdo	13	25,0	25,0	42,3
De acuerdo	16	30,8	30,8	73,1
Totalmente de acuerdo	14	26,9	26,9	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

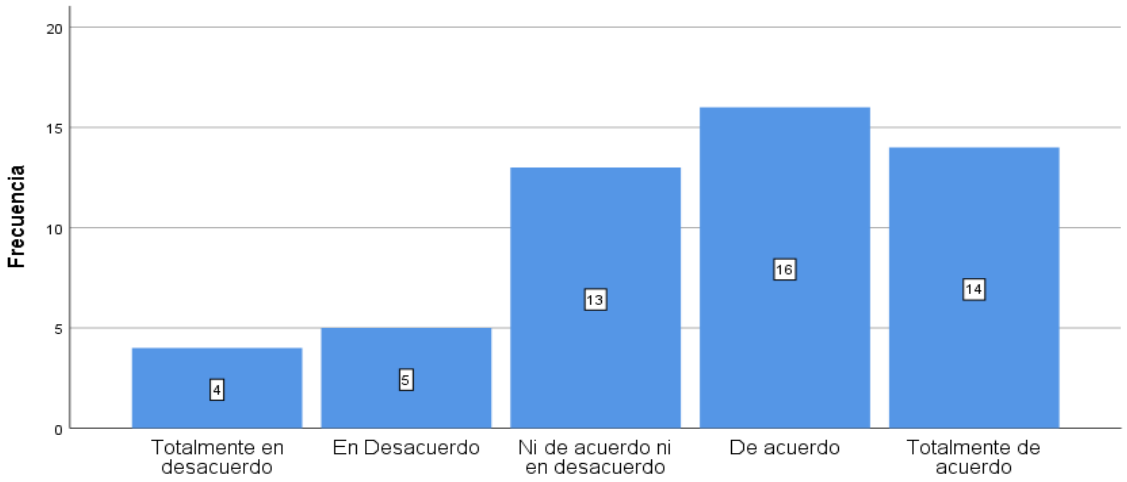


Figura 26. Post Prueba - La cooperación consiente de un usuario en un ataque informático que no afecta el proceso de autenticación.

Se evalúa que el 30.8 % que corresponde a 16 de 52 colaboradores de la población encuestada alude que está de acuerdo, mientras que el 9.6 % está en desacuerdo respecto a que la cooperación del usuario en forma consiente dentro de un ataque informático no afecta el proceso de autenticación.

Dimensión 3: Auditoria Seguridad

Tabla 30: Post Prueba - El proceso de autenticación permite asegurar la identidad veraz de una persona asociado a la cuenta con la que accedió.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	2	3,8	3,8	3,8
En Desacuerdo	4	7,7	7,7	11,5
Ni de acuerdo ni en desacuerdo	6	11,5	11,5	23,1
De acuerdo	21	40,4	40,4	63,5
Totalmente de acuerdo	19	36,5	36,5	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

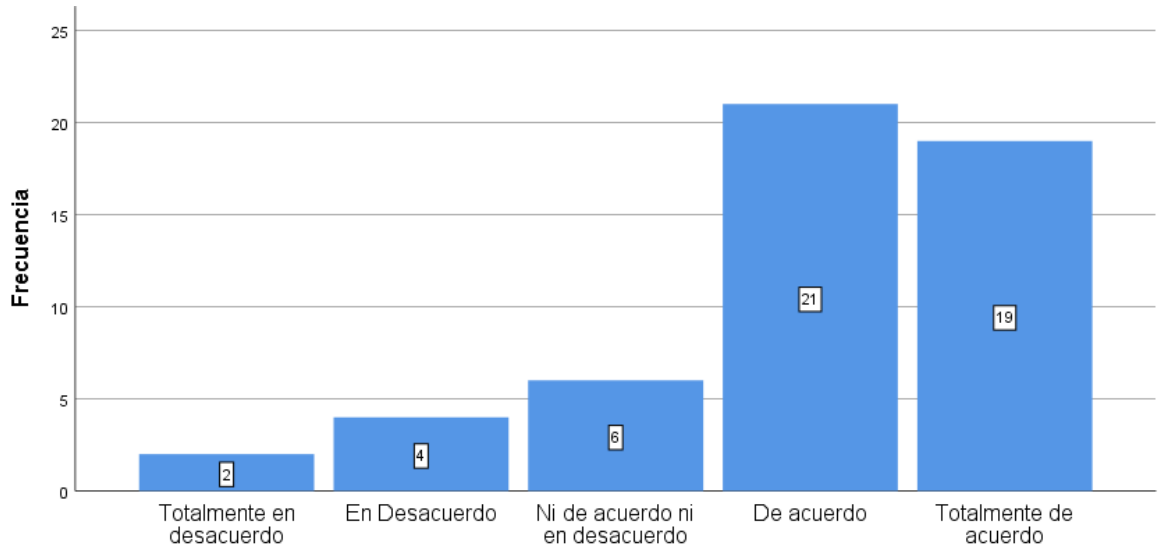


Figura 27. Post Prueba - El proceso de autenticación permite asegurar la identidad veraz de una persona asociado a la cuenta con la que accedió.

Se aprecia que el 40.4 % que referencia a 21 de 52 colaboradores de la población encuestada está de acuerdo, mientras que el 7.7 % está en desacuerdo respecto a que el proceso de autenticación permite asegurar de forma veraz la identidad de una persona asociada a la cuenta con la que accedió.

Tabla 31: Post Prueba El proceso de autenticación permite llevar un registro de actividad confiable de los usuarios dentro del sistema.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	5	9,6	9,6	9,6
En Desacuerdo	7	13,5	13,5	23,1
Ni de acuerdo ni en desacuerdo	10	19,2	19,2	42,3
De acuerdo	18	34,6	34,6	76,9
Totalmente de acuerdo	12	23,1	23,1	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

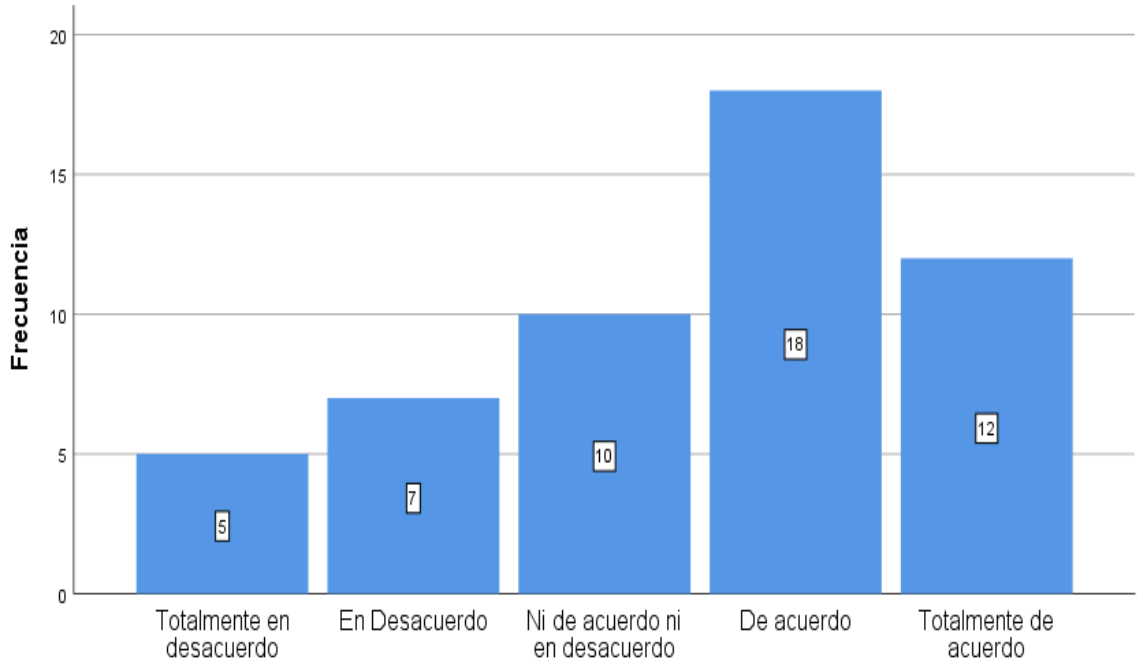


Figura 28. Post Prueba El proceso de autenticación permite llevar un registro de actividad confiable de los usuarios dentro del sistema.

Se observa que el 34.6 % de la población encuestada revela que está de acuerdo, mientras que el 13.5 % está en desacuerdo, respecto a que el proceso de autenticación permite llevar un registro de actividad confiable de los usuarios dentro del sistema.

Se precisa como referencia que 18 de 52 colaboradores están de acuerdo de que la autenticación permite asegurar de forma veraz la identidad de una persona de acuerdo con la cuenta asociada con la que accedió

Tabla 32: Post Prueba - El proceso de autenticación de usuarios permite minimizar la ruptura de credenciales de acceso.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	6	11,5	11,5	11,5
En Desacuerdo	7	13,5	13,5	25,0
Ni de acuerdo ni en desacuerdo	17	32,7	32,7	57,7
De acuerdo	9	17,3	17,3	75,0
Totalmente de acuerdo	13	25,0	25,0	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

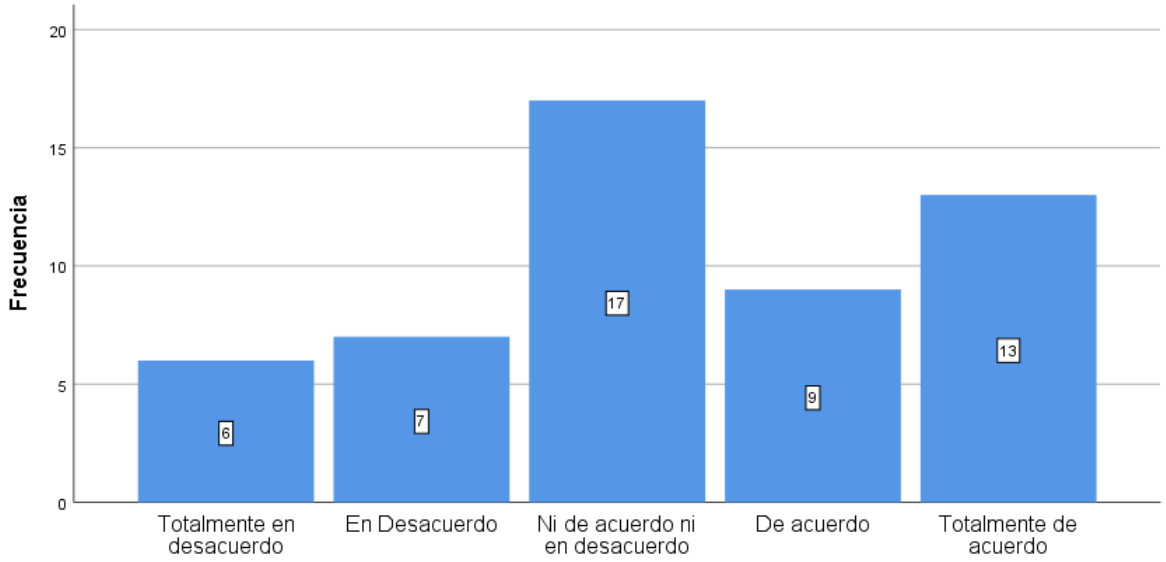


Figura 29. Post Prueba - El proceso de autenticación de usuarios permite minimizar la ruptura de credenciales de acceso.

Se observa que el 13.5 % de la población encuestada revela que está en desacuerdo, mientras que el 17.3 % está de acuerdo correspondientemente, en relación a que el proceso de autenticación de usuarios permite minimizar la ruptura de credenciales de acceso.

Se precisa como referencia que 9 y 13 de 52 colaboradores están de acuerdo y totalmente de acuerdo respectivamente en que el proceso de autenticación permite minimizar la ruptura de credenciales de acceso.

Tabla 33: Post Prueba - La autenticación de usuarios no está sujeto al robo de credenciales.

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en desacuerdo	3	5,8	5,8	5,8
En Desacuerdo	3	5,8	5,8	11,5
Ni de acuerdo ni en desacuerdo	10	19,2	19,2	30,8
De acuerdo	21	40,4	40,4	71,2
Totalmente de acuerdo	15	28,8	28,8	100,0
Total	52	100,0	100,0	

Fuente: Elaboración Propia.

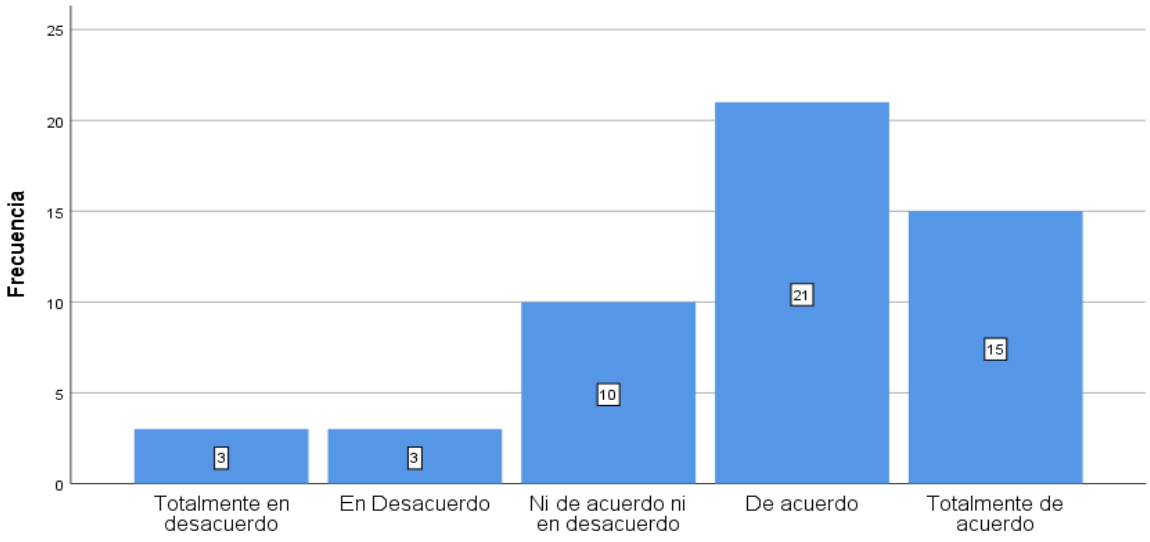


Figura 30. Post Prueba - La autenticación de usuarios no está sujeto al robo de credenciales.

Se observa que el 40.4 % de la población encuestada revela que está de acuerdo, mientras que el 5.8 % está en desacuerdo, orientado a que la autenticación de usuarios no está sujeto al robo de credenciales.

Se señala como referencia que 21 de 52 colaboradores están de acuerdo de que la autenticación de usuarios no está sujeto al robo de credenciales.

4.2. Contrastación de hipótesis

4.2.1. Hipótesis principal

La aplicación de un modelo de Reconocimiento Biométrico por Huella Dactilar si influye en la Seguridad Lógica en Sedapal, 2020.

Para probar esta hipótesis se planteó las siguientes hipótesis de trabajo:

Ho: La aplicación de Reconocimiento Biométrico por Huella Dactilar no influye en la Seguridad Lógica en Sedapal, 2020.

H1: La aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en la Seguridad Lógica en Sedapal, 2020.

Para realizar la docimasia se utilizó la prueba de rangos con signos de Wilcoxon, la cual es una prueba utilizada en variables cualitativas ordinales como lo fue en esta investigación.

Tabla 34: Estadísticos de tendencia central - Pre Prueba

		Total Pre Prueba	Total Post Prueba
N	Válido	52	52
	Perdidos	0	0
Media		30,5192	53,1923
Mediana		30,0000	53,5000
Moda		30,00	56,00
Suma		1587,00	2766,00

Fuente: Elaboración Propia.

Tabla 35: Datos de frecuencia - Pre Prueba

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	23,00	1	1,9	1,9	1,9
	24,00	3	5,8	5,8	7,7
	25,00	2	3,8	3,8	11,5
	26,00	1	1,9	1,9	13,5
	27,00	5	9,6	9,6	23,1
	28,00	5	9,6	9,6	32,7
	29,00	3	5,8	5,8	38,5
	30,00	7	13,5	13,5	51,9
	31,00	6	11,5	11,5	63,5
	32,00	3	5,8	5,8	69,2
	33,00	6	11,5	11,5	80,8
	34,00	3	5,8	5,8	86,5
	36,00	1	1,9	1,9	88,5
	37,00	3	5,8	5,8	94,2
	38,00	2	3,8	3,8	98,1
	39,00	1	1,9	1,9	100,0
	Total	52	100,0	100,0	

Fuente: Elaboración Propia

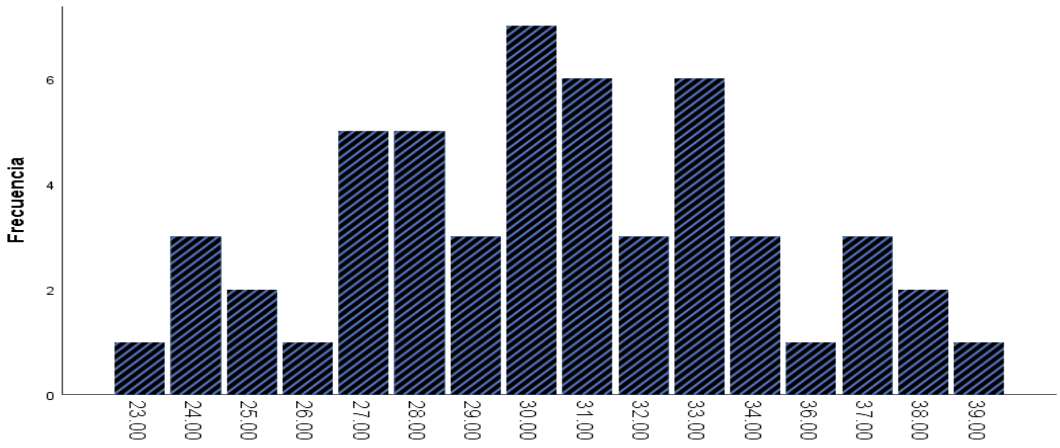


Figura 31. Datos de frecuencia - Pre Prueba.

Tabla 36: Datos de frecuencia – Post Prueba

POST PRUEBA

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	39,00	1	1,9	1,9	1,9
	40,00	2	3,8	3,8	5,8
	44,00	2	3,8	3,8	9,6
	45,00	1	1,9	1,9	11,5
	46,00	1	1,9	1,9	13,5
	47,00	3	5,8	5,8	19,2
	48,00	3	5,8	5,8	25,0
	50,00	2	3,8	3,8	28,8
	51,00	3	5,8	5,8	34,6
	52,00	4	7,7	7,7	42,3
	53,00	4	7,7	7,7	50,0
	54,00	4	7,7	7,7	57,7
	56,00	5	9,6	9,6	67,3
	57,00	2	3,8	3,8	71,2
	58,00	4	7,7	7,7	78,8
	59,00	3	5,8	5,8	84,6
	60,00	3	5,8	5,8	90,4
	61,00	2	3,8	3,8	94,2
	62,00	1	1,9	1,9	96,2
	63,00	1	1,9	1,9	98,1
	64,00	1	1,9	1,9	100,0
	Total	52	100,0	100,0	

Fuente: Elaboración Propia

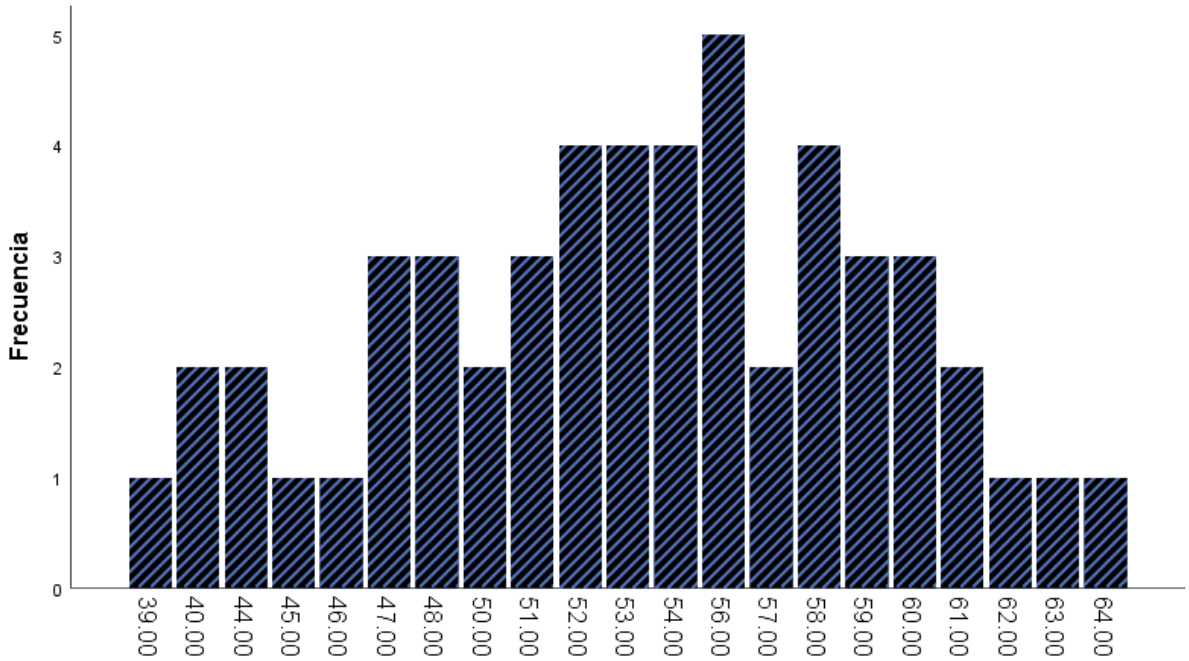


Figura 32. Datos de frecuencia - Post Prueba.

Se observa en la tabla 34 que en la pre prueba se obtuvo una media de 30.51, en contraste con el resultado de la post prueba, la cual obtuvo una media de 53.19, lo que refleja un incremento del 74. 33 % de variación con el pre test, asimismo, de visualizarse un valor alto de influencia del reconocimiento biométrico por huella dactilar en la seguridad lógica.

Tabla 37: Contrastación hipótesis principal

Rangos

		N	*Rango promedio*	*Suma de rangos*
Puntaje de la Post prueba – Puntaje de la Preprueba	*Rangos Negativos*	0[a]	*,00*	*,00*
	Rangos Positivos	52[b]	*47,00*	*4371,00*
	Empates	0[c]		
	Total	*52*		

Fuente: SPSS

a. Puntaje de la Post prueba < Puntaje de la Preprueba

b. Puntaje de la Post prueba > Puntaje de la Preprueba

c. Puntaje de la Post prueba = Puntaje de la Preprueba

Tabla 38: Estadísticos de Prueba - Hipótesis principal.

Estadísticos de prueba

	Puntaje de la Post prueba Seguridad Lógica – Puntaje de la Pre prueba Seguridad Lógica
Z	-8,377[b]
Sig. asintótica (bilateral)	,000

Fuente: SPSS

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Como el nivel de significancia (Significación asintótica bilateral) es 0,000, la cual es menor que 0.05 entonces se rechazó la hipótesis nula:

La aplicación de Biométrico por Huella Dactilar no influye en la Seguridad Lógica en Sedapal, 2020.

Por lo tanto, se acepta la hipótesis alterna:

La aplicación de Biométrico por Huella Dactilar si influye en la Seguridad Lógica en Sedapal, 2020.

De esta manera la investigación concluyó en la comprobación de la hipótesis principal, dando como resultado que la variable interviniente (Reconocimiento Biométrico por Huella Dactilar) sí tiene influencia en la variable dependiente (Seguridad Lógica).

4.2.2. Hipótesis secundarias

Hipótesis secundaria 1

Tabla 39: Estadísticos de tendencia central – Primera dimensión.

		Pre Prueba 1era Dimensión	Post Prueba 1era Dimensión
N	Válido	52	52
	Perdidos	0	0
Media		11,9808	21,4231
Mediana		12,0000	22,0000
Moda		10,00[a]	20,00[a]
Suma		623,00	1114,00

a. Existen múltiples modos. Se muestra el valor más pequeño.

Fuente: Elaboración Propia.

Tabla 40: Datos de frecuencia - Pre Prueba primera dimensión.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	6,00	1	1,9	1,9	1,9
	8,00	1	1,9	1,9	3,8
	9,00	3	5,8	5,8	9,6
	10,00	10	19,2	19,2	28,8
	11,00	8	15,4	15,4	44,2
	12,00	7	13,5	13,5	57,7
	13,00	10	19,2	19,2	76,9
	14,00	5	9,6	9,6	86,5
	15,00	4	7,7	7,7	94,2
	16,00	2	3,8	3,8	98,1
	18,00	1	1,9	1,9	100,0
	Total	52	100,0	100,0	

Fuente: Elaboración Propia.

Tabla 41: Datos de frecuencia - Post Prueba primera dimensión.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	12,00	1	1,9	1,9	1,9
	15,00	2	3,8	3,8	5,8
	16,00	3	5,8	5,8	11,5
	17,00	1	1,9	1,9	13,5
	18,00	1	1,9	1,9	15,4
	19,00	2	3,8	3,8	19,2
	20,00	7	13,5	13,5	32,7
	21,00	7	13,5	13,5	46,2
	22,00	7	13,5	13,5	59,6
	23,00	7	13,5	13,5	73,1
	24,00	7	13,5	13,5	86,5
	25,00	2	3,8	3,8	90,4
	26,00	4	7,7	7,7	98,1
	27,00	1	1,9	1,9	100,0
	Total	52	100,0	100,0	

Fuente: Elaboración Propia.

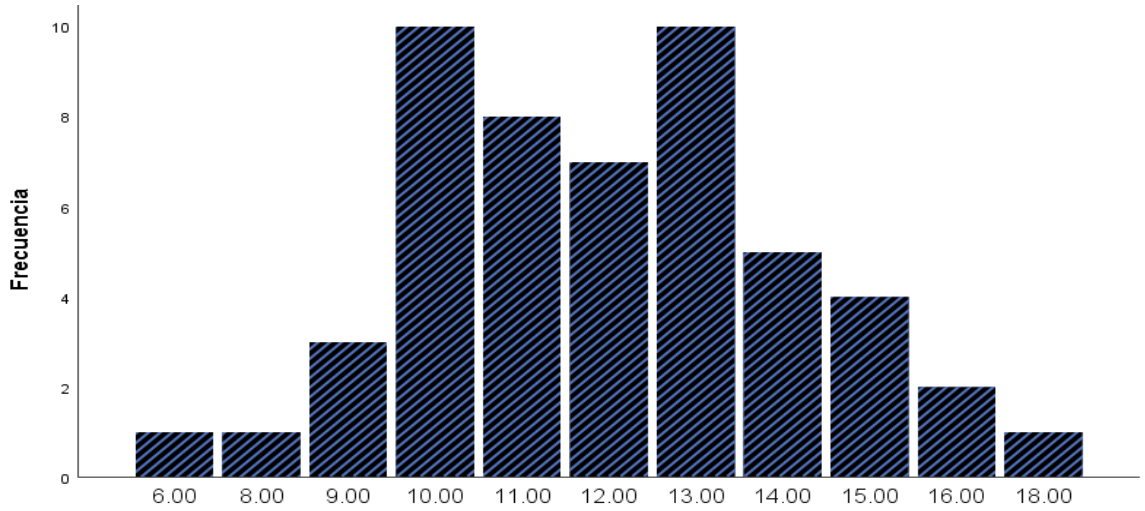


Figura 33. Datos de frecuencia - Pre Prueba primera dimensión.

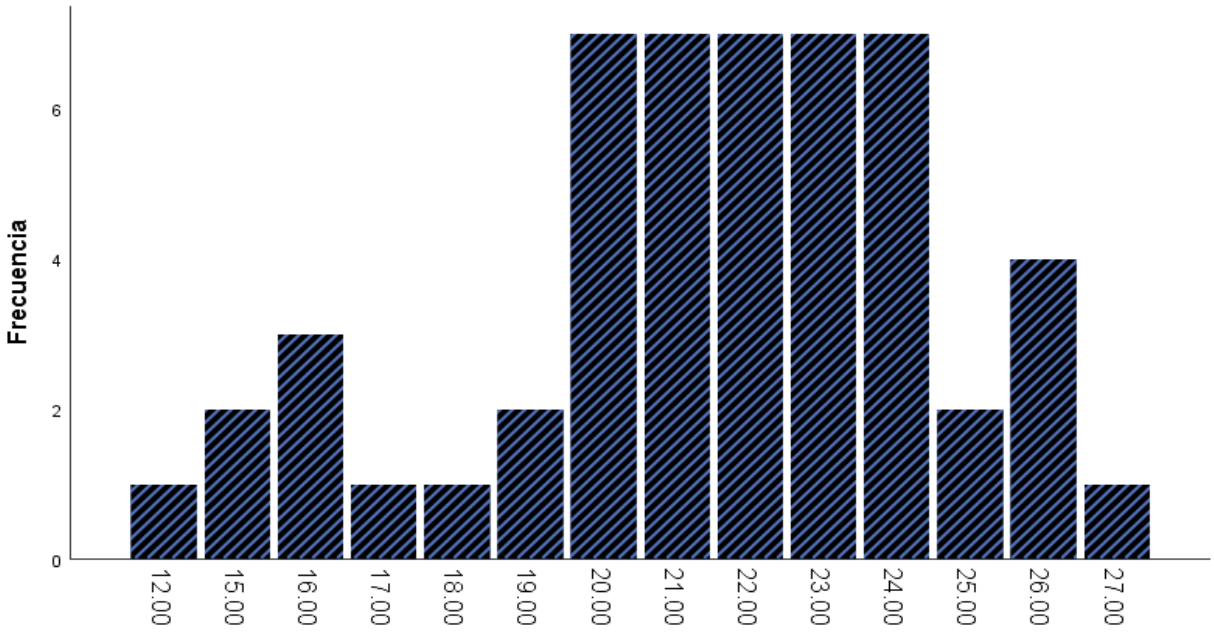


Figura 34. Datos de frecuencia - Post Prueba primera dimensión.

Se observa en la tabla 39 que en la pre prueba se obtuvo una media de 11.98, en contraste con el resultado de la post prueba, la cual obtuvo una media de 21.42, lo que refleja un incremento del 78. 79 % de variación con el pre test, asimismo, de

visualizarse un valor alto de influencia del reconocimiento biométrico por huella dactilar en el control de acceso.

La aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en el Control de Acceso en Sedapal, 2020.

Para probar esta hipótesis se planteó las siguientes hipótesis de trabajo:

Ho: La aplicación de Reconocimiento Biométrico por Huella Dactilar no influye en el Control de Acceso en Sedapal, 2020.

H1: La aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en el Control de Acceso en Sedapal, 2020.

Tabla 42: Estadísticos de prueba –Hipótesis secundaria 1

Estadísticos de prueba

Puntaje de la Post prueba Control de Acceso– Puntaje de la Pre prueba Control de Acceso	
Z	-8,362[b]
Sig. asintótica (bilateral)	,000

Fuente: SPSS

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Como el nivel de significancia (Significación asintótica bilateral) es 0,000, la cual es menor que 0.05 entonces se rechazó la hipótesis nula:

La aplicación de Biométrico por Huella Dactilar no influye en el Control de Acceso en Sedapal, 2020.

Por lo tanto, se acepta la hipótesis alterna:

La aplicación de Biométrico por Huella Dactilar si influye en el Control de Acceso en Sedapal, 2020.

De esta manera la investigación concluyó en la comprobación de la hipótesis secundaria 1, dando como resultado que el Reconocimiento Biométrico por Huella Dactilar sí tiene influencia en el Control de acceso en Sedapal.

Hipótesis secundaria 2

Tabla 43: Estadísticos de tendencia central - Segunda dimensión.

		Pre Prueba 2da Dimensión	Post Prueba 2da Dimensión
N	Válido	52	52
	Perdidos	0	0
Media		10,4615	17,1923
Mediana		11,0000	17,5000
Moda		9,00	19,00
Suma		544,00	894,00

Fuente: Elaboración Propia.

Tabla 44: Datos de frecuencia - Pre Prueba segunda dimensión.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	6,00	1	1,9	1,9	1,9
	7,00	6	11,5	11,5	13,5
	8,00	4	7,7	7,7	21,2
	9,00	10	19,2	19,2	40,4
	10,00	4	7,7	7,7	48,1
	11,00	9	17,3	17,3	65,4
	12,00	6	11,5	11,5	76,9
	13,00	8	15,4	15,4	92,3
	14,00	2	3,8	3,8	96,2
	15,00	1	1,9	1,9	98,1
	16,00	1	1,9	1,9	100,0
	Total	52	100,0	100,0	

Fuente: Elaboración Propia.

Tabla 45: Datos de frecuencia - Post Prueba segunda dimensión.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	11,00	3	5,8	5,8	5,8
	12,00	1	1,9	1,9	7,7
	13,00	1	1,9	1,9	9,6
	14,00	4	7,7	7,7	17,3
	15,00	7	13,5	13,5	30,8
	16,00	4	7,7	7,7	38,5
	17,00	6	11,5	11,5	50,0
	18,00	6	11,5	11,5	61,5
	19,00	8	15,4	15,4	76,9
	20,00	5	9,6	9,6	86,5
	21,00	6	11,5	11,5	98,1
	23,00	1	1,9	1,9	100,0
	Total	52	100,0	100,0	

Fuente: Elaboración Propia.

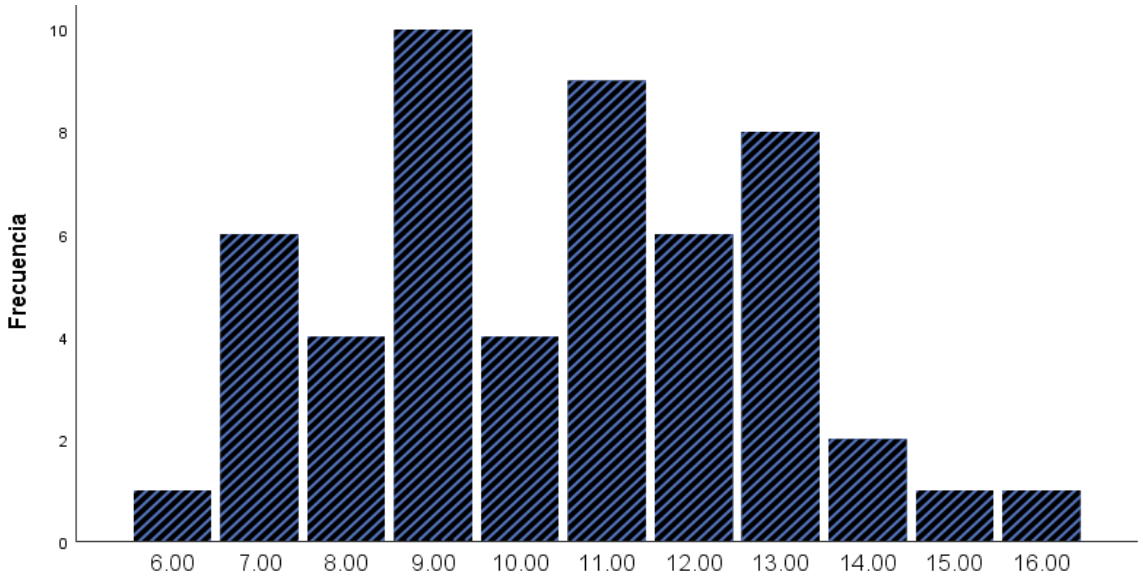


Figura 35. Datos de frecuencia – Pre prueba segunda dimensión

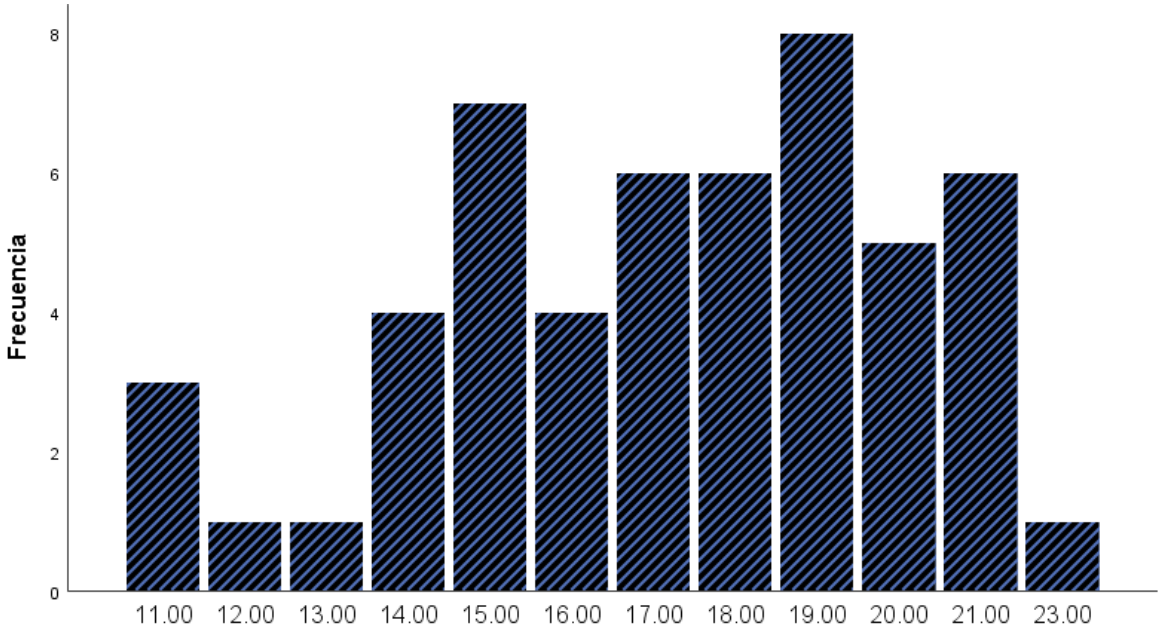


Figura 36. Datos de frecuencia – Post prueba segunda dimensión

La aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en la Ingeniería Social en Sedapal, 2020.

Para probar esta hipótesis se planteó las siguientes hipótesis de trabajo:

Ho: La aplicación de Reconocimiento Biométrico por Huella Dactilar no influye en la Ingeniería Social en Sedapal, 2020.

H1: La aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en la Ingeniería Social en Sedapal, 2020.

Tabla 46: Estadísticos de prueba –Hipótesis secundaria 2

Estadísticos de prueba

	Puntaje de la Post prueba Ingeniería Social – Puntaje de la Pre prueba Ingeniería Social
Z	-8,322[b]
Sig. asintótica (bilateral)	,000

Fuente: SPSS

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Como el nivel de significancia (Significación asintótica bilateral) es 0,000, la cual es menor que 0.05 entonces se rechazó la hipótesis nula:

La aplicación de Biométrico por Huella Dactilar no influye en la Ingeniería Social en Sedapal, 2020.

Por lo tanto, se acepta la hipótesis alterna:

La aplicación de Biométrico por Huella Dactilar si influye en la Ingeniería Social en Sedapal, 2020.

De esta manera la investigación concluyó en la comprobación de la hipótesis secundaria 2, dando como resultado que el Reconocimiento Biométrico por Huella Dactilar sí tiene influencia en la Ingeniería Social en Sedapal.

Hipótesis secundaria 3

Tabla 47: Estadísticos de tendencia central - Tercera dimensión.

		Pre Prueba 3era Dimensión	Post Prueba 3era Dimensión
N	Válido	52	52
	Perdidos	0	0
Media		8,0385	14,5769
Mediana		8,0000	15,0000
Moda		6,00	17,00
Suma		418,00	758,00

Fuente: Elaboración Propia.

Tabla 48: Datos de frecuencia - Pre Prueba tercera dimensión.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	5,00	1	1,9	1,9	1,9
	6,00	13	25,0	25,0	26,9
	7,00	10	19,2	19,2	46,2
	8,00	10	19,2	19,2	65,4
	9,00	6	11,5	11,5	76,9
	10,00	4	7,7	7,7	84,6
	11,00	5	9,6	9,6	94,2
	12,00	3	5,8	5,8	100,0
	Total	52	100,0	100,0	

Fuente: Elaboración Propia.

Tabla 49: Datos de frecuencia - Post Prueba tercera dimensión.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	7,00	1	1,9	1,9	1,9
	9,00	2	3,8	3,8	5,8
	10,00	2	3,8	3,8	9,6
	11,00	3	5,8	5,8	15,4
	12,00	2	3,8	3,8	19,2
	13,00	9	17,3	17,3	36,5
	14,00	2	3,8	3,8	40,4
	15,00	8	15,4	15,4	55,8
	16,00	7	13,5	13,5	69,2

	17,00	11	21,2	21,2	90,4
	18,00	3	5,8	5,8	96,2
	19,00	2	3,8	3,8	100,0
	Total	52	100,0	100,0	

Fuente: Elaboración Propia.

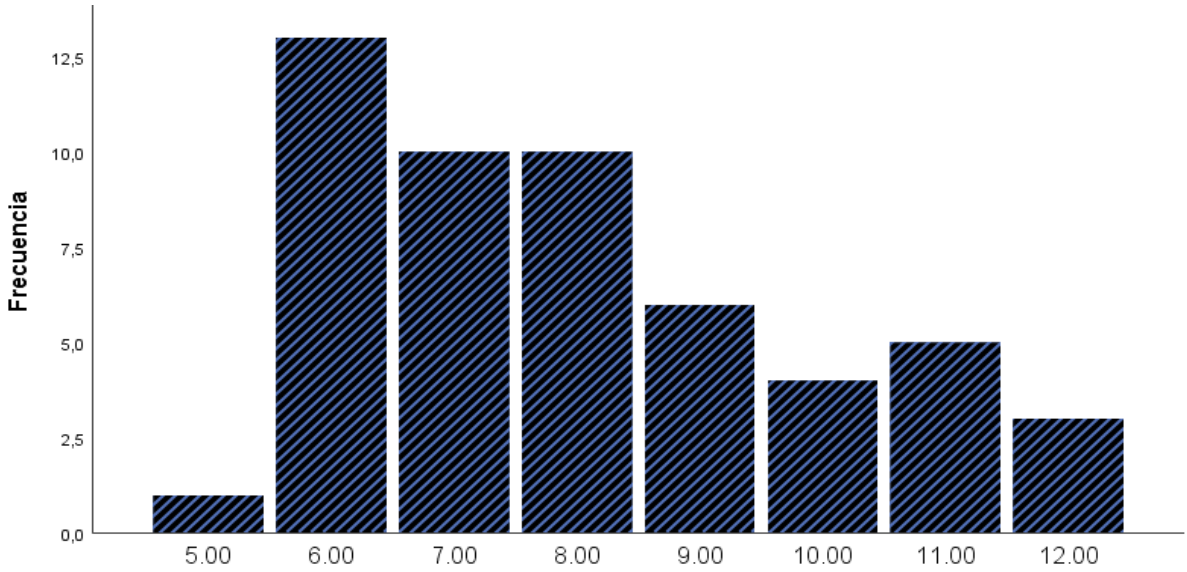


Figura 37. Datos de frecuencia – Pre prueba tercera dimensión

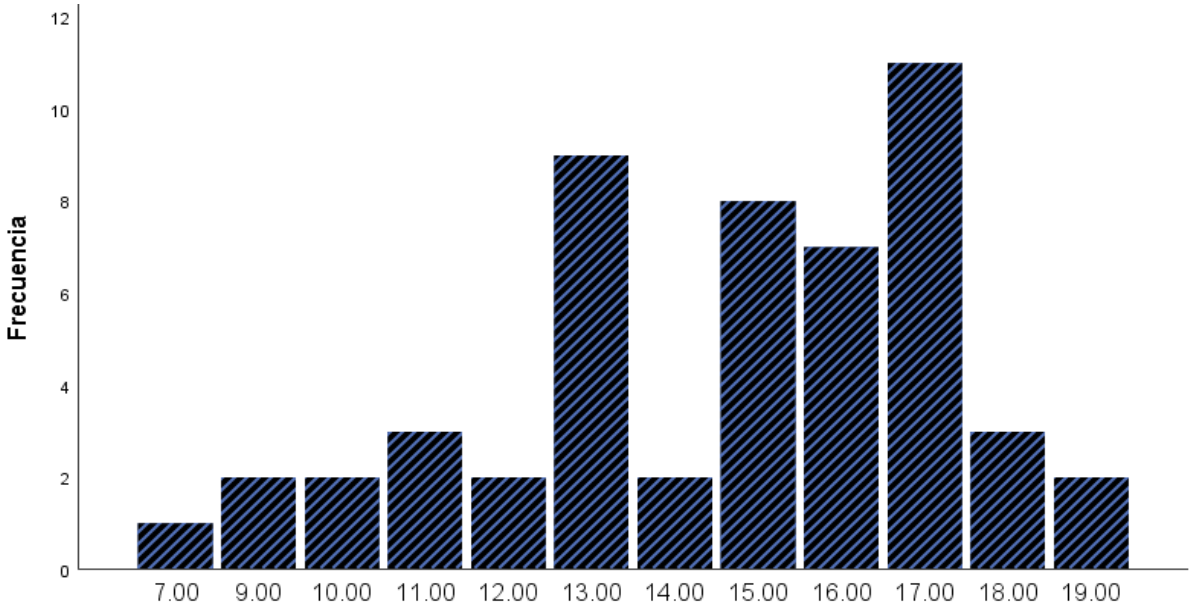


Figura 38. Datos de frecuencia – Post prueba tercera dimensión

La aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en la Auditoria de Seguridad en Sedapal, 2020.

Para probar esta hipótesis se planteó las siguientes hipótesis de trabajo:

Ho: La aplicación de Reconocimiento Biométrico por Huella Dactilar no influye en la Auditoria de Seguridad en Sedapal, 2020.sdp

H1: La aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en la Auditoria de seguridad en Sedapal, 2020.

Tabla 50: Estadísticos de prueba –Hipótesis secundaria 3

Estadísticos de prueba

Puntaje de la Post prueba Auditoria de seguridad – Puntaje de la Pre prueba Auditoria de seguridad	
Z	-8,120[b]
Sig. asintótica (bilateral)	,000

Fuente: SPSS

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Como el nivel de significancia (Significación asintótica bilateral) es 0,000, la cual es menor que 0.05 entonces se rechazó la hipótesis nula:

La aplicación de Biométrico por Huella Dactilar no influye en la Auditoria de seguridad en Sedapal, 2020.

Por lo tanto, se acepta la hipótesis alterna:

La aplicación de Biométrico por Huella Dactilar si influye en la Auditoria de Seguridad en Sedapal, 2020.

De esta manera la investigación concluyó en la comprobación de la hipótesis secundaria 3, dando como resultado que el Reconocimiento Biométrico por Huella Dactilar sí tiene influencia en el Auditoria de seguridad en Sedapal.

V. DISCUSIÓN

En la presente investigación se planteó como propósito mostrar la influencia que tiene la Aplicación de un modelo de Reconocimiento Biométrico por Huella Dactilar en la Seguridad Lógica en SEDAPAL; para ello se comparó los resultados obtenidos en esta investigación con los resultados y conclusiones obtenidos de los antecedentes. A continuación, se discute los principales hallazgos.

1. Según Monjaraz (2015) en su tesis de investigación, realizada en Perú en Universidad Científica del Sur, titulada: “Estudio de pre factibilidad para implementar biometría mediante huella digital en la red de cajeros automáticos, Banco de Crédito del Perú”, alcanzando el resultado de intervalos de confianza sólidos, concluye que los sistemas biométricos son la mejor alternativa en el país para lograr una correcta y rápida autenticación, aumentando considerablemente la seguridad, además argumenta que la innovación tecnológica debe ir acompañada de procesos internos adecuados, añadiendo que el personal esté debidamente capacitado para poder llevarlo adelante.

En comparación con la investigación mencionada en el párrafo anterior, en teoría está enfocada para un uso masivo al igual que la presente investigación, la diferencia incurre en la centralización del público objetivo y en el tratamiento de la tecnología, es decir, SEDAPAL posee una rigurosa gestión con la finalidad de garantizar la seguridad de su información a través de medidas preventivas y correctivas, sin embargo no concibe los intervalos de confianza necesarios para las necesidades y exigencias actuales, se posee una estructura sólida y organizada pero carece de las políticas para correlacionar la tecnología biométrica con sus procesos organizacionales

Por otro lado, se rescata que existe personal comprometido, que se encuentra inmerso en los procesos de la organización, concibiendo las causas y consecuencias que pondrían en riesgo a la empresa, por lo cual se puede lograr una convergencia de recursos que conlleven al cumplimiento del alcance y demanda de los objetivos pertinentes para esta tecnología.

2. Según Marín (2017) en su investigación, realizada en Perú, en la Universidad Tecnológica del Perú, titulada: “Propuesta de mejora de un sistema biométrico

multiusuario para cajeros automáticos en instituciones bancarias en la ciudad de lima - 2017", concluye que la realización del sistema influye principalmente para tener los mejores resultados, ya que sin un buen bosquejo de seguridad con todas las bases de datos de los clientes principales y/o secundarios, no se puede obtener un buen nivel de reconocimiento facial, también indicó que los sistemas biométricos no son perfectos al 100% considerando que estos actualmente son la mejor alternativa en el país para lograr una correcta y rápida autenticación, aumentando considerablemente la seguridad.

En ese sentido, se puede comprometer la calidad en el procesamiento del sistema, si es que las etapas que la conforman no cumplen con los criterios necesarios para garantizar el correcto funcionamiento de la tecnología, es muy importante concebir el concepto de calidad total de inicio a fin, respetando los intervalos externos y cumpliendo con una recopilación de recursos adecuados, asumiendo como parte fundamental la información que existe de por medio.

3. Según Llatas (2015) en su tesis de investigación, en la Pontifica Universidad Católica del Perú, titulada: "El registro biométrico dactilar con el sistema AFIS y el control del delito", con el objetivo de analizar la implementación del sistema AFIS y determinar el impacto que tienen en la identificación certera de personas involucradas en un acto delictivo. Concluye que se requiere de personal que este correctamente capacitado para su manejo.

De acuerdo a lo mencionado, el compromiso y la alta capacidad del personal a cargo de la tecnología biométrica es fundamental para una efectiva Gestión de la seguridad de la información, sin embargo es importante precisar que las constantes charlas y programas de consentimiento orientados a garantizar y cumplir con los aspectos fundamentales de la seguridad que establece SEDAPAL, respaldado por las políticas y estándares corporativos, deben están sujetas a un constante control y mejora continua.

4. Según Inoguchi y Macha (2015) en su tesis de investigación en Perú, en la Universidad San Ignacio de Loyola, titulada: *"*Gestión de la ciberseguridad de los

ataques cibernéticos en las PYMES del Perú", con el objetivo de determinar la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, 2016. Concluye que La Empresa Zavala Cargo S.A.C. tiene una falta del uso de planes contra ataques de Seguridad Cibernética, que resguarden su información cibernética permitiendo así una toma de decisiones más confiable, además agregó la falta de apoyo económico al proceso de creación de medidas de seguridad informática dentro de una red privada, provocando así que la organización se exponga a mayores riesgos.

En comparación con la Empresa Zavala Cargo S.A.C, SEDAPAL cuenta con un equipo especializado en el tratamiento de incidencias de seguridad, hechos que pueden comprometer la seguridad de la información y el conjunto de elementos que derivan para el correcto funcionamiento de los diversos procesos correlacionados a la misma; se posee grupos funcionales dedicados a prevenir, analizar, corregir y recuperar de acuerdo a los diversas tipologías que puedan poner en riesgo o comprometer los intereses del equipo. Por otro lado, existe una supervisión contante por parte de las áreas interesadas, con el fin de garantizar la correcta aplicación de procedimientos, además de brindarle un acercamiento contante a la realidad actual, orientado a la mejora continua de sus procesos y cumplimiento de sus objetivos de gestión

5. Según Hernández (2016) en su investigación, realizada en México, en la Universidad Autónoma del Estado de México, titulada: "Autenticación biométrica a través de huellas digitales e iris en una empresa industrial", concluye que, la necesidad de tener un sistema de seguridad ya sea para control de acceso o autenticación de individuo ha llevado estar buscando nuevas alternativas de sistemas, además menciona que los sistemas al no recurrir al uso de claves personalizadas, tarjetas, llaves, entre otras los cuales son fácilmente de robar o clonar, sino al proceso de autenticar biométricamente con iris y huella dactilar, otorga una mayor confiabilidad en la seguridad.

De acuerdo a la presente investigación, se ha mencionado la eficacia de los sistemas de acceso por claves, pero la interminable lista de desventajas que ponen en riesgo los objetivos principales de la seguridad. Por otro lado, se evaluó las necesidades

socioeconómicas de la Empresa SEDAPAL, así como la delicada e importante tarea de mantener y asegurar la confiabilidad e integridad de la información, no solo por el hecho de brindar un servicio público, sino por garantizar la seriedad y profesionalismo orientado a brindar un servicio con el respaldo de procesos y recursos concebidos con una gestión efectiva de calidad total.

6. Según Montaña (2017) en su investigación, realizada en Colombia, en la Universidad Libre Sede Bosque Popular, titulada: “Sistema de identificación mediante huella digital para el control de accesos a la Universidad Libre Sede Bosque Popular simulado en un entorno web”, con el objetivo de desarrollar un sistema de identificación por huella digital para control de accesos de la Universidad Libre Sede Bosque Popular simulado en un entorno web. Esta Tesis se centra en el análisis respectivo en la manera de cómo se deben utilizar los recursos tecnológicos para lograr el cumplimiento de los objetivos de este proyecto.

Por otra parte, las aplicaciones de SEDAPAL l, son concebidas en un entorno cerrado dentro de una red corporativa, la cual no la hace menos propensa a ataques y/o amenazas informáticas, pero es importante mencionar que tanto en un entorno público como privado el manejo de los recursos es imprescindible para la efectividad del recurso y sus fines. SEDAPAL posee unos procedimientos periódicos de auditoria, la cual no solo incurre en supervisar el cumplimiento de los procesos sino en el correcto uso de los recursos intervinientes.

7. Vallejo y Carrera (2017) realizó una investigación en Ecuador, en la Escuela Superior Politécnica de Chimborazo, titulada: “Implementación de un sistema biométrico de huellas dactilares para el control de asistencia estudiantil en la escuela de Ingeniería Industrial de la Facultad de Mecánica”, concluye que al implementar los equipos biométricos y el software attendance management se automatizó el proceso de control de asistencia tradicional, además que se seleccionó el software Attendance Management por sus amplias características que permitieron cumplir con la programación deseada, obteniendo reportes de asistencia de una manera rápida, segura y eficiente.

Se concibe la idea enfocada a señalar a los equipos biométricos como una tecnología efectiva para sus fines, pero es importante mencionar que todo recurso orientado a salvaguardar la información, actualmente es muy asequible a ser comprometida, no solo por agentes externos, sino por los mismos usuarios que por una acción de descuido o conciencia inmoral ponen en riesgo los fundamentos principales de la seguridad. Por lo tanto, es necesario el seguimiento y control adecuado, aplicando medidas de prevención y emplear una medida correctiva si el caso amerita, para de esta manera exigir el cumplimiento total de los procedimientos de seguridad.

8. Según Sánchez (2015) en su investigación, consolidada en España, en la Universidad Carlos III de Madrid, titulada: “Estudio del rendimiento biométrico de sistemas de huella dactilar. Análisis de diferentes sensores y algoritmos”, concluye que se ha implementado correctamente una aplicación capaz de realizar las comparaciones de varias muestras obtenidas con tres sensores distintos y bajo el uso de dos algoritmos diferentes.

El mercado biométrico es diverso y varía de acuerdo a niveles de complejidad algorítmica y estructural, así como diferentes escalas económicas; lo importante es precisar las necesidades que la organización requiere para cada proceso, categorizándolo por niveles de importancia y riesgo, además de mantener una implementación escalable y permanente con miras a alcanzar la excelencia total.

Por otro lado, es imprescindible que el criterio de evaluación del recurso sea de acuerdo a referencia técnicas orientadas al funcionamiento efectivo y de rendimiento absoluto para garantizar la seguridad de la información y sus fines con la organización y sus intereses.

VI. CONCLUSIONES

1. La aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en la Seguridad Lógica en SEDAPAL, 2020, donde al contrastarse utilizando la prueba de rangos con signos de Wilcoxon, la cual es una prueba empleada en variables cualitativas ordinales para muestras relacionadas, resultó con un nivel de significación de 0,000 menor que 0,05, quedando rechazada la hipótesis nula y aceptando la alterna.

2. La aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en el Control de Acceso en SEDAPAL, 2020, donde al contrastarse utilizando la prueba de rangos con signos de Wilcoxon, la cual es una prueba empleada en variables cualitativas ordinales para muestras relacionadas, resultó con un nivel de significación de 0,000 menor que 0,05, quedando rechazada la hipótesis nula y aceptando la alterna.

3. La aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en la Ingeniería Social en SEDAPAL, 2020, donde al contrastarse utilizando la prueba de rangos con signos de Wilcoxon, la cual es una prueba aplicada en variables cualitativas ordinales para muestras relacionadas, resultó con un nivel de significación de 0,000 menor que 0,05, quedando rechazada la hipótesis nula y aceptando la alterna.

4. La aplicación de un modelo de Reconocimiento Biométrico por Huella Dactilar si influye en la Auditoria de seguridad en SEDAPAL, 2020, donde al contrastarse utilizando la prueba de rangos con signos de Wilcoxon, la cual es una prueba empleada en variables cualitativas ordinales para muestras relacionadas, resultó con un nivel de significación de 0,000 menor que 0,05, quedando rechazada la hipótesis nula y aceptando la alterna.

5. Por otro lado, el diseño de investigación pre experimental aplicado, el cual expresa que tiene un grado de control mínimo en orientación a que únicamente se trabajó con un solo grupo, además que se analizó una sola variable y no existió la posibilidad de comparación de grupos, añadiendo que la muestra seleccionada de 52 colaboradores de la empresa SEDAPAL fue de manera intencional, debido a ciertos factores socioeconómicos y relacionados con la seguridad interna de la organización, como

también la accesibilidad a una mayor cantidad muestral de la población, por lo cual los resultados obtenidos representan parcialmente a la población general de la empresa, sin embargo la presente investigación y sus resultados favorables pueden ser usados como una base fundamental de primer acercamiento al problema de investigación planteado, para que posteriormente se empleé un diseño más consolidado y confiable, con la conformación de grupos de comparación que aporten criterios situacionales por niveles, para que de esta forma se determine un mayor margen de generalización teniendo como base los resultados positivos obtenidos en esta investigación.

VII. RECOMENDACIONES

Se recomienda lo siguiente:

1. Conformar una investigación más profunda enfocada a persistir en la consolidación y aseguramiento total de la información, a partir de procedimientos y estructuras que permitan obtener resultados que garanticen la sostenibilidad corporativa y que se orienten a los objetivos de primer nivel.

2. Mantener una orientación organizativa y una evaluación de los requerimientos de acuerdo a las necesidades fundamentales de la empresa, manteniendo como prioridad la satisfacción total del cliente, como también integra la información relacionada a su servicio.

3. En lo que respecta a la aplicación de una tecnología biométrica en la Gestión de la seguridad, debe ser implementada de manera progresiva y de acuerdo a las necesidades reales de cada usuario relacionado con el tipo de información que maneja, además de evaluar los niveles de riesgo y sensibilidad de datos. Un análisis más exhaustivo orientado a las políticas de seguridad brindaría una guía global efectiva para la correcta superación de problemas vigentes relacionada con la seguridad.

4. Es importante la capacitación constante, como también charlas de concientización sobre el adecuado uso de herramientas encaminadas a respaldar y proteger la información. Para ello, se debe emplear una estrategia comunicativa dentro del entorno laboral para determinar las necesidades latentes y de esa manera planificar capacitaciones que resulten beneficiosas para la productividad de la empresa.

5. En los procesos de auditoria se debe contar con un registro histórico veraz de las actividades, incidencias y/o observaciones encontradas, con la finalidad que se garantice la evaluación de las medidas de prevención, además de supervisar que se cumplan con todos los procedimientos con miras al resguardo de la información y sus fines, asimismo de garantizar la protección de los intereses de la corporación.

VIII. REFERENCIAS

Aguilera, P. (2011). *Seguridad Informática*. Madrid, España: Editorial Editex S.A.

Aldegani, G. (1997). *Seguridad Informática*. Buenos Aires, Argentina: Editorial MP Ediciones.

Álvarez, G. & Pérez, P. (2004). *Seguridad Informática para empresas y particulares.* Madrid, España: McGraw-Hill/Interamericana de España, S. A. U.

Araujo, I. & Linares, E. (2018). *Desarrollo de aplicaciones biométricas y cognitivas para un modelo de espejo inteligente* (Tesis de pregrado). Universidad Peruana de Ciencias Aplicadas, Perú.

Asociación de Examinadores de Fraude Certificados (2019). *Tecnología antifraude ¿La están usando las empresas?* Madrid, España: Asociación contra el fraude. Recuperado de https://asociacioncontraelfraude.com/tecnologia-anti-fraude/

Auditoría, Consejo, Instalación y Seguridad de Sistemas de Información (2015). *Seguridad Informática Hacking Ético conocer el ataque para una mejor defensa.* Barcelona, España: ENI.

Banco Bilbao Vizcaya Argentaria (2016). *Tecnología Biométrica*. Madrid, España: Centro de innovación BBVA. Recuperado de https://www.bbva.com/wp-content/uploads/2017/10/ebook-cibbva-biometria-pc.pdf

Benchimol, D. (2011). *Hacking desde cero*. Buenos Aires, Argentina: Fox Andina S.A.

Boulgouris, V, Plataniotis, N. & Tzanakou, E (2010). *Biometrics: Theory, Methods, and Applications.* Estados Unidos: Wiley-IEEE Press.

Carrasco, S. (2007). *Metodología de la Investigación Científica*. Lima, Perú: San Marcos E.I.R.L.

Carri, J., Pasini, A. Pesado, P., & Giusti, A. (2007). *Reconocimiento biométrico en aplicaciones de E-Government: Análisis de confiabilidad / tiempo de respuesta.* Revista XIII Congreso Argentino de Ciencias de la Computacion. pp. 497 - 506 Recuperado de: http://sedici.unlp.edu.ar/bitstream/handle/10915/22014/Documento_completo.pdf?sequence=1&isAllowed=y

Córdova, C., & Santana, C. (2011). *¿Cómo las tomas de decisiones se apoyan en los sistemas de información?* Panamá, Panamá.

Das, R. (2015). *Biometric technology Biography, cloud-based architecture*. New York, Estados Unidos: CRC Press Taylor & Francis Group.

De Pablos, C., López, J., Romo, S. & Medina, S. (2019). *Organización y trasformación de los sistemas de información en la empresa* (4ta ed.). Madrid, España: ESIC Editorial.

Escajedo, L. (2015). *Reconocimiento e identificación de las personas mediante Biometrías estáticas y dinámicas (*Tesis doctoral). Universidad de Alicante, España.

Escrivá, G., Romero, R., Ramada, D. & Onrubia, R. (2013). *Seguridad Informática.* España: Macmillan Profesional.

ESET Security (2016). *ESET Security Report Latinoamerica 2016*. Welive security. Recuperado de https://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf

Fundación Telefónica (2016). *Ciberseguridad, la protección de la información en un mundo digital.* Barcelona, España: Ariel, S.A.

Gómez, A. (2011). *Enciclopedia de la Seguridad Informática*. Madrid, España: Ra-Ma.

González, P. (2014). *Ethical Hacking: Teoría practica para la realización de un pentesting.* Madrid, España: 0xWord Computing.

Hernández, J. (2016). *Autenticación biométrica a través de huellas digitales e iris en una empresa industrial (*Tesis de pregrado). Universidad Autónoma del Estado de México, México.

Hernández, J. & Flórez, J. (2011). *Seguridad física y lógica en el manejo de la información policial.* Revista Logos, Ciencia & Tecnología, 3(1), pp. 222-233. Recuperado de https://www.redalyc.org/pdf/5177/517751801016.pdf.

Huidobro, J. & Roldan, D. (2005). *Seguridad en Redes y Sistemas Informáticos*. Madrid, España: Thomson Paraninfo.

Inoguchi, A. & Macha, E. (2017). *Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las pymes del Perú, 2016 (*Tesis de pregrado). Universidad San Ignacio de Loyola, Perú.

Instituto del Mar del Perú (2012). *Políticas de seguridad informática y comunicaciones-PSIC*. Lima, Perú: IMARPE. Recuperado de https://cdn.www.gob.pe/uploads/document/file/355813/Resoluci%C3%B3n_Directoral_N__DE-143-201220190827-2102-4reaxn.pdf

Instituto Nacional de Estadística e Informática (2001). *Delitos Informáticos.* Lima, Perú: INEI

Instituto Nacional de Tecnologías de la Comunicación (2011). *Estudio sobre las tecnologías biométricas aplicada a la seguridad*. León, España: INTECO.

Jain, A., Flynn, P. & Ross, A. (2008). *Handbook of Biometrics.* Estados Unidos: Springer.

Jara, H. y García, F. (2015). *Ethical Hacking 2.0.* Buenos Aires, Argentina: Fox Andina S.A & Dagala S.A

Kaspersky (2018). *¿Qué es la biometría?* México: Kaspersky Latam. Recuperado de https://latam.kaspersky.com/resource-center/definitions/biometrics

Komarinski, P. (2004). *Automated fingerprint identification systems*. Estados Unidos: Elsevier Academic Press.

Llatas, O. (2016). *El registro biométrico dactilar con el sistema AFIS y el control del delito (*Tesis de pos grado). Pontificia Universidad Católica del Perú, Perú.

Marcel, S., Nixon, M. & Li, S. (2014). *Handbook of Biometric Anti-Spoofing.* Estados Unidos: Springer.

Marín, J. (2017). *Propuesta de mejora de un sistema biométrico multiusuario para cajeros automáticos en instituciones bancarias en la ciudad de lima - 2017* (Tesis de pre grado). Universidad Tecnológica del Perú, Perú.

Martos, F., Desongles, J., Santos, M., & González, J. (2004). *Auxiliares Administrativos de la Diputación Provincial de Huelva.* España, Sevilla: MAD, SL.

Monjaraz, C. (2015). *Estudio de pre factibilidad para implementar biometría mediante huella digital en la red de cajeros automáticos, banco de crédito del Perú* (Tesis de pre grado). Universidad Científica del Sur, Perú.

Montaña, D. (2017). *Sistema de identificación mediante huella digital, para el control de accesos a la Universidad Libre Sede Bosque Popular simulado en un entorno web* (Tesis de pre grado). Universidad Libre Sede Bosque Popular, Colombia.

Oficina Nacional de Tecnologías de Información (2005). *Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional.* Buenos Aires, Argentina: ONTI

Ortega, F., Fernández, F. & Coomonte, R. (2008). *Biometría y Seguridad*. Madrid, España: Universidad Autónoma de Madrid.

Portantier, F. (2012). *Seguridad Informática.* Buenos Aires, Argentina: Fox Andina S.A & Dagala S.A

Ramos, A., Barbero, C., Marugán, D. y González, I. (2015). *Hacking con Ingeniería Social, Técnicas para hackear humanos.* Madrid, España: Ra-Ma

Registro Nacional de Identificación y Estado Civil (2010). *Servicio de verificación biométrica - SVB.* Lima, Perú: RENIEC. Recuperado de http://www.reniec.gob.pe/portal/pdf/05_svb.pdf.

Sabino, C. (1992). El proceso de la investigación. Caracas, Venezuela: Panapo.

Sánchez, S. (2015). *Estudio del rendimiento Biométrico de Sistemas de Huella Dactilar. Análisis de diferentes sensores y algoritmos* (Tesis de pre grado). Universidad Carlos III de Madrid, España.

Serratosa, F. (2012). *La biometría para la identificación de las personas*. Madrid, España: Universidad Autónoma de Madrid.

Silva, F., Segadas, L. & Kowask, E. (2014). *Gestión de la seguridad de la información*. Bogotá, Colombia: Redcedia. Recuperado de https://cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI8.pdf

Simón, D. (2003). *Reconocimiento automático mediante patrones biométricos de huellas dactilares* (Tesis Doctoral). Universidad Politécnica de Madrid. España.

Solé, A. (2013). *Seguridad en los sistemas biométricos*. Barcelona, España: Eureca Media, SL.

Vallejo, P. y Carrera, A. (2017). *Implementación de un sistema biométrico de huellas dactilares para el control de asistencia estudiantil en la Escuela de Ingeniería Industrial de la Facultad de Mecánica* (Tesis de pre grado). Escuela Superior Politécnica de Chimborazo, Ecuador.

Virtual Instrument Software Architecture (2016). *Los españoles confían en la banca para la biometría del futuro*. Madrid, España: Diario el Comercio. Recuperado de https://www.visa.es/sobre-la-corporacion-visa/sala-de-prensa-de-visa/press-releases.1568002.html

Yeliseyev, S. (2016). *Biometría es el medio que más seguridad y privacidad ofrece*. Lima, Perú: Diario el Comercio. Recuperado de https://elcomercio.pe/economia/negocios/biometria-medio-seguridad-privacidad-ofrece-274795-noticia/

IX. ANEXOS

Anexo 1: Matriz de Consistencia

<table>
<tr><th>Problema General</th><th>Objetivo General</th><th>Hipótesis General</th><th>Variables y Dimensiones</th><th>Diseño Metodológico</th></tr>
<tr><td>• ¿De qué manera influye la Aplicación de Reconocimiento Biométrico por Huella Dactilar en la Seguridad Lógica en SEDAPAL, 2020?</td><td>• Determinar qué manera influye la Aplicación de Reconocimiento Biométrico por Huella Dactilar en la Seguridad Lógica en SEDAPAL, 2020.</td><td>• La Aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en la Seguridad Lógica en SEDAPAL, 2020.</td><td rowspan="3">Variable Independiente
Reconocimiento Biométrico por Huella Dactilar

Variable Dependiente
Seguridad lógica

-Dimensiones
• Control de acceso
• Ingeniería social
• Auditoria de seguridad</td><td rowspan="3">Tipo: Aplicada
Diseño: Experimental - Pre experimental
Nivel: Experimental
Población:
52 trabajadores del Equipo de Clientes Especiales de SEDAPAL.
Muestra:
Muestra censal, los 52 trabajadores del Equipo de Clientes Especiales de SEDAPAL.
Técnicas e instrumentos de recolección de datos:
Técnica: Encuesta y fichaje
Instrumento:
Cuestionario</td></tr>
<tr><td>Problemas Específicos</td><td>Objetivos Específicos</td><td>Hipótesis Secundaria</td></tr>
<tr><td>a) ¿De qué manera influye la Aplicación de Reconocimiento Biométrico por Huella Dactilar en el Control de Acceso en SEDAPAL, 2020?
b) ¿De qué manera influye la Aplicación de Reconocimiento Biométrico por Huella Dactilar en la Ingeniería Social en SEDAPAL, 2020?
c) ¿De qué manera influye la Aplicación de Reconocimiento Biométrico por Huella Dactilar en la Auditoria de Seguridad en SEDAPAL, 2020?</td><td>a) Explicar de qué manera influye la Aplicación de Reconocimiento Biométrico por huella dactilar en el Control de Acceso en SEDAPAL, 2020.
b) Describir de qué manera influye la Aplicación de Reconocimiento Biométrico por huella dactilar en la Ingeniería Social en SEDAPAL, 2020.
c) Mencionar de qué manera influye la Aplicación de Reconocimiento Biométrico por huella dactilar en la Auditoria de Seguridad en SEDAPAL, 2020.</td><td>a) La Aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en el Control de Acceso en SEDAPAL, 2020.
b) La Aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en la Ingeniería Social en SEDAPAL, 2020.
c) La Aplicación de Reconocimiento Biométrico por Huella Dactilar si influye en la Auditoria de Seguridad en SEDAPAL, 2020.</td></tr>
</table>

Anexo 2: Matriz de Operacionalización de la Variable Dependiente

Variable	Dimensiones	Indicadores	Ítems	Escala de Medición
Seguridad Lógica	Control de Acceso	Eficiencia	1, 2	Escala Likert. 5 = Totalmente de acuerdo 4 = De acuerdo 3 = Ni de acuerdo ni en desacuerdo 2 = En desacuerdo 1 = Totalmente en desacuerdo
		Seguridad de acceso	3, 4	
		Gestión de credenciales	5, 6	
	Ingeniería Social	Amenaza	7, 8	
		Ataque	9	
		Cooperación	10, 11	
	Auditoria de Seguridad	Confiabilidad	12, 13	
		Accesibilidad	14, 15	

Anexo 3: Instrumento

CUESTIONARIO DE LA TESIS

TESIS: APLICACIÓN DE RECONOCIMIENTO BIOMÉTRICO POR HUELLA DACTILAR Y SU INFLUENCIA EN LA SEGURIDAD LOGICA EN SEDAPAL, 2020

Nombre y Apellidos:

……

DNI N°: …… Teléfono/Celular: ..……

Instrucción / Empresa:

……..

Sexo: Hombre ( ) Mujer ( )

Edad: 18-22 ( ) 23-25 ( ) 26-30 ( ) 31-40 ( ) 40 a más ( )

Valora de acuerdo a la siguiente escala:

(1) En desacuerdo
(2) Totalmente en desacuerdo
(3) Ni de acuerdo ni en desacuerdo
(4) De acuerdo
(5) Totalmente de acuerdo

Dimensiones / Ítems					
Dimensión 1: Control de Acceso					
1. No resulta tedioso a los usuarios ingresar las credenciales de acceso a los programas informáticos.					
2. El tiempo para el proceso de autenticación es optimo					
3. La autenticación de usuarios a los programas informáticos es segura					
4. El proceso de autenticación permite el acceso a una cuenta solo a la persona autorizada					

5. Las credenciales de acceso de los usuarios no tienden a ser olvidadas					
6. La cantidad de credenciales asignadas a los usuarios para acceder a los programas informáticos es adecuada.					
Dimensión 2: Ingeniería Social					
7. El descuido del usuario no representa una amenaza para el proceso de autenticación.					
8. El espionaje corporativo no es una amenaza difícil de detectar en el proceso de autenticación de usuarios.					
9. El proceso de autenticación no es propenso a un ataque por manipulación de personas.					
10. El proceso de autenticación limita a los usuarios compartir sus credenciales con otras personas.					
11. La cooperación consiente de un usuario en un ataque informático que no afecta el proceso de autenticación.					
Dimensión 3: Auditoria de Seguridad					
12. El proceso de autenticación permite asegurar la identidad veraz de una persona asociado a la cuenta con la que accedió					
13. El proceso de autenticación permite llevar un registro de actividad confiable de los usuarios dentro del sistema.					
14. El proceso de autenticación de usuarios permite minimizar la ruptura de credenciales de acceso					
15. La autenticación de usuarios no está sujeto al robo de credenciales					

Anexo 4: Validación del Instrumento

FORMATO B

FICHAS DE VALIDACIÓN DEL INFORME DE OPINIÓN POR JUICIO DE EXPERTO

I. DATOS GENERALES

1.1. Título de la Investigación : Aplicación de un Modelo de Reconocimiento Biométrico por Huella Dactilar y su influencia en la Seguridad Lógica en Sedapal, 2019.

1.2. Nombre del instrumento: Cuestionario sobre Recolección de Información

II. ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Está formulado con leguaje apropiado																				X
2. Objetividad	Está expresado en conductas observables																				X
3. Actualidad	Adecuado al avance de la ciencia pedagógica																				X
4. Organización	Existe una organización Lógica																			X	
5. Suficiencia	Comprende los aspectos en cantidad y calidad																				X
6. Intencionalidad	Adecuado para valorar los instrumentos de Investigación																				X
7. Consistencia	Basado en aspectos teóricos científicos																			X	
8. Coherencia	Entre los índices e indicadores																				X
9. Metodología	La estrategia responde al propósito del diagnóstico																				X
10. Pertinencia	Es útil y adecuado para la investigación																			X	

	Baja
	Regular
	Buena
	Muy buena

PROMEDIO DE VALORACIÓN
OPINIÓN DE APLICABILIDAD

98.5

RECOMENDACIONES:

.....

.....

PROMEDIO DE VALORACIÓN

OPINIÓN DE APLICABILIDAD

a) Deficiente b) Baja c) Regular d) Buena e) Muy buena

Nombres Apellidos: WILLIAM MIGUEL MOGROVEJO COLLANTES

DNI N°: 08467408 Teléfono/Celular: 994981897

Dirección domiciliaria: URB. EL PACÍFICO CALLE AUGUSTO SALAZAR BONDY N° 2052

Título Profesional: INGENIERO DE SISTEMAS CIP 153999

Grado Académico: DOCTORADO

Mención: DOCTOR EN EDUCACIÓN

Firma

Lugar y fecha: LIMA, 03 DE JUNIO 2019

UNIVERSIDAD PRIVADA TELESUP

Dr. Ing. CIP William Mogrovejo Collantes
Defensoría Universitaria
UNIVERSIDAD PRIVADA TELESUP

FORMATO B

FICHAS DE VALIDACIÓN DEL INFORME DE OPINIÓN POR JUICIO DE EXPERTO

I. DATOS GENERALES

1.1. Título de la Investigación : Aplicación de un Modelo de Reconocimiento Biométrico por Huella Dactilar y su influencia en la Seguridad Lógica en Sedapal, 2019.

1.2. Nombre del instrumento: Cuestionario sobre Recolección de Información

II. ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Está formulado con leguaje apropiado																		✓		
2. Objetividad	Está expresado en conductas observables																		✓		
3. Actualidad	Adecuado al avance de la ciencia pedagógica																		✓		
4. Organización	Existe una organización Lógica																		✓		
5. Suficiencia	Comprende los aspectos en cantidad y calidad																		✓		
6. Intencionalidad	Adecuado para valorar los instrumentos de investigación																		✓		
7. Consistencia	Basado en aspectos teóricos científicos																		✓		
8. Coherencia	Entre los índices e indicadores																		✓		
9. Metodología	La estrategia responde al propósito del diagnóstico																		✓		
10. Pertinencia	Es útil y adecuado para la investigación																		✓		

	Baja
	Regular
✓	Buena
	Muy buena

PROMEDIO DE VALORACIÓN OPINIÓN DE APLICABILIDAD

90 %

RECOMENDACIONES:

.....

.....

PROMEDIO DE VALORACIÓN

OPINIÓN DE APLICABILIDAD

a) Deficiente b) Baja c) Regular (d) Buena e) Muy buena

Nombres Apellidos: AYBAR HUAMANI, JUSTINIANO

DNI 08874474N°: 08822478 Teléfono/Celular:

.....

Dirección domiciliaria:.....

Título Profesional:

.....

Grado Académico: DOCTOR EN EDUCACIÓN

Mención: CIENCIAS DE LA EDUCACION

Dra. Justiniano, AYBAR HUAMANI
METODÓLOGO Y TEMÁTICO DE TESIS

Lugar y fecha: 2/06/19

FORMATO B

FICHAS DE VALIDACIÓN DEL INFORME DE OPINIÓN POR JUICIO DE EXPERTO

I. DATOS GENERALES

1.1. Título de la Investigación : Aplicación de un Modelo de Reconocimiento Biométrico por Huella Dactilar y su influencia en la Seguridad Lógica en Sedapal, 2019.

1.2. Nombre del instrumento: Cuestionario sobre Recolección de Información

II. ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Está formulado con leguaje apropiado																				X
2. Objetividad	Está expresado en conductas observables																			X	
3. Actualidad	Adecuado al avance de la ciencia pedagógica																				X
4. Organización	Existe una organización Lógica																			X	
5. Suficiencia	Comprende los aspectos en cantidad y calidad																				X
6. Intencionalidad	Adecuado para valorar los instrumentos de investigación																				X
7. Consistencia	Basado en aspectos teóricos científicos																				X
8. Coherencia	Entre los índices e indicadores																				X
9. Metodología	La estrategia responde al propósito del diagnóstico																			X	
10. Pertinencia	Es útil y adecuado para la investigación																				X

	Baja
	Regular
	Buena
	Muy buena

PROMEDIO DE VALORACIÓN OPINIÓN DE APLICABILIDAD	98.5

RECOMENDACIONES:

.....

.....

PROMEDIO DE VALORACIÓN

OPINIÓN DE APLICABILIDAD

a) Deficiente b) Baja c) Regular d) Buena (e) Muy buena

Nombres Apellidos: EDWIN HUGO BENAVENTE ORELLANA

DNI 10626370 N°: ..... Teléfono/Celular: 992207743

Dirección domiciliaria: CALLAO – LIMA

Título Profesional: ING SISTEMAS

Grado Académico: MAGISTER

Mención: ADM DE NEGOCIOS / ING SISTEMAS

EDWIN HUGO
BENAVENTE ORELLANA
INGENIERO DE SISTEMAS
Reg. CIP N° 124728

Firma

Lugar y fecha: LIMA 07/06/2019

Anexo 5: Matriz de Datos

Niveles y Rangos	Bajo	Medio	Alto	Muy alto
Seguridad Logica	[15 - 29]	[30 - 44]	[45 - 59]	[60 - 75]
Control de Acceso	[6 - 11]	[12 - 17]	[18 - 23]	[24 - 30]
Ingenieria Social	[5 - 9]	[10 - 14]	[15 - 19]	[20 -25]
Auditoria de seguridad	[4 - 7]	[8 - 11]	[12 - 15]	[16 - 20]

PRE PRUEBA DE LA VARIABLE DEPENDIENTE SEGURIDAD LOGICA																		
CONTROL DE ACCESO							INGENIERIA SOCIAL						AUDITORIA INFORMATICA					TOTAL
Preg. 1	Preg. 2	Preg. 3	Preg. 4	Preg. 5	Preg. 6	TOTAL	Preg. 7	Preg. 8	Preg. 9	Preg. 10	Preg. 11	TOTAL	Preg. 12	Preg. 13	Preg. 14	Preg. 15	TOTAL	GENER.
2	1	2	2	2	4	13	1	4	3	4	2	14	4	4	1	1	10	37
2	2	2	2	2	2	12	1	2	1	2	4	10	3	1	2	1	7	29
1	1	2	2	1	2	9	3	2	2	1	3	11	1	3	2	2	8	28
3	2	1	2	3	1	12	3	1	1	4	4	13	3	3	1	1	8	33
1	2	3	1	1	3	11	2	3	4	2	1	12	2	2	3	4	11	34
2	1	1	3	2	1	10	2	1	3	2	1	9	2	2	1	3	8	27
2	2	2	1	2	2	11	1	2	2	4	3	12	2	1	2	2	7	30
2	1	2	2	2	2	11	3	2	2	1	3	11	1	3	2	2	8	30
1	2	2	2	1	2	10	1	2	1	1	2	7	3	1	2	1	7	24
2	2	1	2	2	1	10	2	1	3	5	2	13	1	3	3	1	8	31
2	2	2	1	2	3	12	2	3	1	2	1	9	2	2	1	1	6	27
2	1	2	2	2	1	10	2	1	2	2	3	10	2	2	4	1	9	29
1	3	2	2	1	2	11	1	2	2	1	1	7	2	1	2	1	6	24
2	1	2	2	2	2	11	2	2	2	3	2	11	2	3	2	2	9	31
2	1	1	1	2	2	9	2	2	1	3	1	9	1	3	1	1	6	24
2	2	3	3	2	1	13	2	1	1	2	1	7	2	1	3	4	10	30
4	3	1	1	4	2	15	1	2	3	2	2	10	2	2	1	3	8	33
3	3	2	2	3	2	15	2	2	3	1	1	9	1	1	2	2	6	30
2	2	2	2	2	2	12	2	2	2	3	4	13	3	4	2	2	11	36
3	2	2	2	2	1	12	2	1	2	1	3	9	1	1	2	1	5	26
3	2	1	1	1	2	10	4	2	1	2	2	11	2	3	2	2	9	30
4	1	2	3	2	3	15	3	2	3	2	2	12	2	3	1	1	7	34
2	2	3	3	2	3	15	2	2	1	1	2	8	1	2	3	4	10	33
3	2	3	4	2	4	18	1	4	3	3	2	13	2	2	1	3	8	39
2	1	4	2	2	2	13	3	3	2	3	1	12	1	1	2	2	6	31
1	1	2	3	3	3	13	3	3	2	2	3	13	4	3	2	2	11	37
3	3	3	2	3	2	16	4	4	4	2	1	15	3	1	2	1	7	38
1	1	2	1	4	1	10	5	2	1	2	1	11	2	3	1	1	7	28
2	2	1	3	2	3	13	3	3	3	2	2	13	2	2	3	4	11	37
1	2	3	1	3	1	11	2	2	3	1	1	9	1	2	1	3	7	27
2	1	1	2	2	2	10	1	1	2	3	4	11	1	2	1	2	6	27
2	2	2	1	1	1	9	3	3	2	1	3	12	3	2	2	2	9	30
1	1	1	2	3	2	10	3	1	1	2	2	9	3	1	1	1	6	25
3	3	2	3	3	2	16	4	5	3	2	2	16	2	1	2	1	6	38
2	3	2	3	3	1	14	2	1	1	2	1	7	2	3	2	2	9	30
1	1	1	4	4	3	14	3	2	3	2	3	13	1	3	1	1	6	33
1	1	3	2	2	2	11	2	2	2	1	2	9	3	2	3	4	12	32
2	3	2	3	3	1	14	1		1	3	2	7	1	2	1	3	7	28
1	3	1	2	2	1	10	3	3	3	1	1	11	4	1	2	1	8	29
1	1	1	1	1	1	6	1	2	1	2	3	9	1	3	2	2	8	23
2	2	1	3	1	2	11	2	1	2	1	2	8	1	3	1	1	6	25
2	1	1	1	1	2	8	1	1	1	3	2	8	2	2	3	4	11	27
4	2	2	1	2	1	12	2	2	2	3	5	14	1	2	1	3	7	33
4	1	2	1	5	1	14	2	2	2	2	3	11	4	1	2	2	9	34
2	2	2	2	3	2	13	1	1	1	2	1	6	3	5	2	2	12	31
1	3	4	2	1	2	13	3	3	3	1	2	12	2	1	2	1	6	31
3	1	2	2	1	4	13	2	1	2	3	1	9	2	1	1	2	6	28
1	2	1	4	3	3	14	1	1	1	1	3	7	2	2	2	1	7	28
1	3	3	2	1	2	12	1	3	1	3	5	13	1	2	1	2	6	31
3	1	1	1	3	1	10	2	1	2	1	2	8	3	2	2	3	10	28
1	2	1	3	1	5	13	2	3	1	3	2	11	3	1	1	3	8	32
3	3	3	1	2	1	13	2	1	2	1	1	7	2	3	4	3	12	32

POST PRUEBA DE LA VARIABLE DEPENDIENTE SEGURIDAD LOGICA																		
CONTROL DE ACCESO							INGENIERIA SOCIAL						AUDITORIA INFORMATICA					TOTAL
Preg. 16	Preg. 17	Preg. 18	Preg. 19	Preg. 20	Preg. 21	TOTAL	Preg. 22	Preg. 23	Preg. 24	Preg. 25	Preg. 26	TOTAL	Preg. 27	Preg. 28	Preg. 29	Preg. 30	TOTAL	GENER.
3	5	4	4	4	4	24	3	1	4	4	3	15	4	4	2	4	14	53
4	5	4	4	2	5	24	4	5	4	4	3	20	5	4	3	4	16	60
2	4	4	5	4	4	23	2	4	4	5	5	20	5	2	4	5	16	59
4	5	3	5	5	4	26	4	5	3	5	2	19	4	4	4	3	15	60
3	3	4	2	3	5	20	3	3	4	2	4	16	2	4	3	2	11	47
2	5	2	2	4	5	20	2	1	2	2	4	11	4	4	1	4	13	44
5	3	4	4	3	4	23	5	3	4	4	2	18	4	1	3	5	13	54
2	3	5	4	4	5	23	2	3	5	4	1	15	5	2	3	5	15	53
4	5	5	2	5	4	25	4	5	5	2	4	20	4	4	1	4	13	58
3	2	4	4	2	4	19	3	2	4	4	2	15	4	5	5	3	17	51
4	4	2	4	5	5	24	4	4	2	4	3	17	4	4	3	4	15	56
2	4	4	4	2	4	20	2	4	4	4	4	18	2	1	2	2	7	45
5	2	2	1	1	4	15	5	2	2	1	4	14	4	5	4	4	17	46
3	1	5	2	2	2	15	3	1	5	2	3	14	5	3	2	1	11	40
5	4	2	3	5	4	23	5	4	2	3	1	15	4	3	5	4	16	54
5	2	3	5	2	4	21	5	2	3	5	3	18	5	3	2	3	13	52
5	3	4	4	5	3	24	5	3	4	4	3	19	4	3	3	3	13	56
3	4	2	1	1	1	12	3	4	2	1	1	11	2	4	5	5	16	39
4	4	3	5	5	3	24	4	4	3	5	5	21	3	5	5	3	16	61
5	3	2	3	5	5	23	5	3	2	3	2	15	1	4	4	3	12	50
4	1	4	3	4	5	21	1	5	2	3	5	16	4	4	1	1	10	47
2	3	5	3	3	4	20	4	2	3	4	4	17	5	4	5	5	19	56
5	3	3	3	4	3	21	2	3	5	5	4	19	1	2	3	4	10	50
3	1	2	4	2	4	16	3	4	4	3	5	19	5	4	3	5	17	52
2	5	3	5	3	2	20	4	2	1	1	3	11	4	5	4	4	17	48
1	3	4	5	4	4	21	4	3	5	3	5	20	3	5	5	4	17	58
3	2	2	5	5	5	22	3	2	3	5	5	18	4	4	3	5	16	56
5	4	4	5	5	4	27	1	1	3	4	4	13	5	3	1	4	13	53
3	2	1	4	4	4	18	3	5	3	5	2	18	4	5	3	5	17	53
3	5	4	4	5	5	26	3	3	3	3	3	15	4	4	5	5	18	59
4	4	2	3	4	4	21	1	2	4	4	5	16	5	4	4	4	17	54
5	4	1	2	5	5	22	5	3	5	5	3	21	4	5	5	4	18	61
3	5	5	4	4	1	22	3	4	5	4	5	21	2	1	3	3	9	52
1	3	4	5	4	4	21	2	2	5	3	4	16	5	3	4	5	17	54
3	5	3	5	2	4	22	4	4	5	5	3	21	5	5	4	3	17	60
5	5	2	3	1	4	20	2	1	4	4	1	12	4	4	3	4	15	47
4	4	5	3	4	5	25	5	4	4	5	3	21	5	3	1	4	13	59
5	2	3	5	4	4	23	2	3	5	4	5	19	5	2	3	5	15	57
3	3	3	4	5	4	22	3	3	4	5	4	19	4	5	3	3	15	56
4	5	5	4	4	4	26	5	5	4	4	5	23	5	3	1	4	13	62
5	3	4	5	4	2	23	3	4	5	4	3	19	3	3	5	5	16	58
4	5	2	1	3	1	16	5	2	1	3	4	15	5	5	3	4	17	48
3	4	2	3	3	1	16	4	2	3	3	5	17	3	4	2	2	11	44
4	5	5	2	3	5	24	5	4	2	3	4	18	5	2	4	4	15	57
4	3	3	3	2	2	17	3	3	3	2	3	14	4	2	2	1	9	40
4	4	5	4	4	3	24	4	5	4	4	4	21	5	5	5	4	19	64
5	1	3	5	4	1	19	1	3	5	4	4	17	3	4	2	3	12	48
5	5	5	1	5	5	26	5	5	1	5	4	20	4	5	3	5	17	63
3	5	3	2	4	4	21	5	3	2	4	5	19	5	3	5	5	18	58
5	4	4	1	3	5	22	4	4	1	3	5	17	5	1	3	4	13	52
5	2	4	2	4	5	22	2	1	2	4	5	14	3	2	5	5	15	51
2	5	1	4	3	5	20	5	1	4	3	4	17	4	1	5	4	14	51

Anexo 6: Solicitud de Aplicación de encuesta.

sedapal

Equipo Servicios y Clientes Especiales

Lima, 9 de setiembre del 2020.

Señor
Gerente General de SEDAPAL
Pablo Aguilera Sánchez

Atención: Angel Noriega Mendoza
Ricardo Uribe Reyes
Asunto: Solicita accionar una encuesta laboral
Referencia: Sustentación de tesis académica

Yo, RICARDO ANTONIO JIMENEZ PRADA, identificado con DNI N° 74607905 y trabajador de la empresa SEDAPAL como Técnico VII, acreditado con ficha 15560 y con ejercicio laboral en la Gerencia Comercial – Equipo Servicios y Clientes Especiales – ESCE, sede Breña, ante usted con mucho respeto me presento y digo:

Que, el suscrito ha realizado sus estudios académicos en la facultad de Ingeniería de sistemas en la Universidad Privada Telesup, siendo a la fecha su estado el de egresado y con el grado de bachiller, y como consecuencia de ello viene realizando las acciones para elaborar su tesis académica con la finalidad que mediante una exposición obtener el grado de Ingeniero en Sistemas.

A lo expuesto señor Gerente, considerando que para culminar mi tesis, tengo la necesidad de llevar a cabo una encuesta de medición referida al comportamiento, asimilación y conformidad de las labores con los sistemas de acceso informáticos que llevan los trabajadores de SEDAPAL en sus funciones de gabinete; y es a mérito de ello, por lo cual le solicito se me sirva otorgar el permiso para poder realizar la encuesta vía virtual a los trabajadores del Equipo Servicios y Clientes Especiales, o en su defecto si hubieran realizado una encuesta con similares características, le solicito que su despacho ordene a quien corresponda, me otorgue copia de la encuesta acordada.

Señor Gerente, estando a su disposición de ser el caso que el suscrito realice una exposición mas detallada de lo solicitado, quedo en usted para que su despacho disponga la fecha, tiempo y hora y modo en que el suscrito accionara la exposición del contenido de lo solicitado.

Sin otro particular, quedo en usted trasladándole mis mejores deseos y parabienes personales.

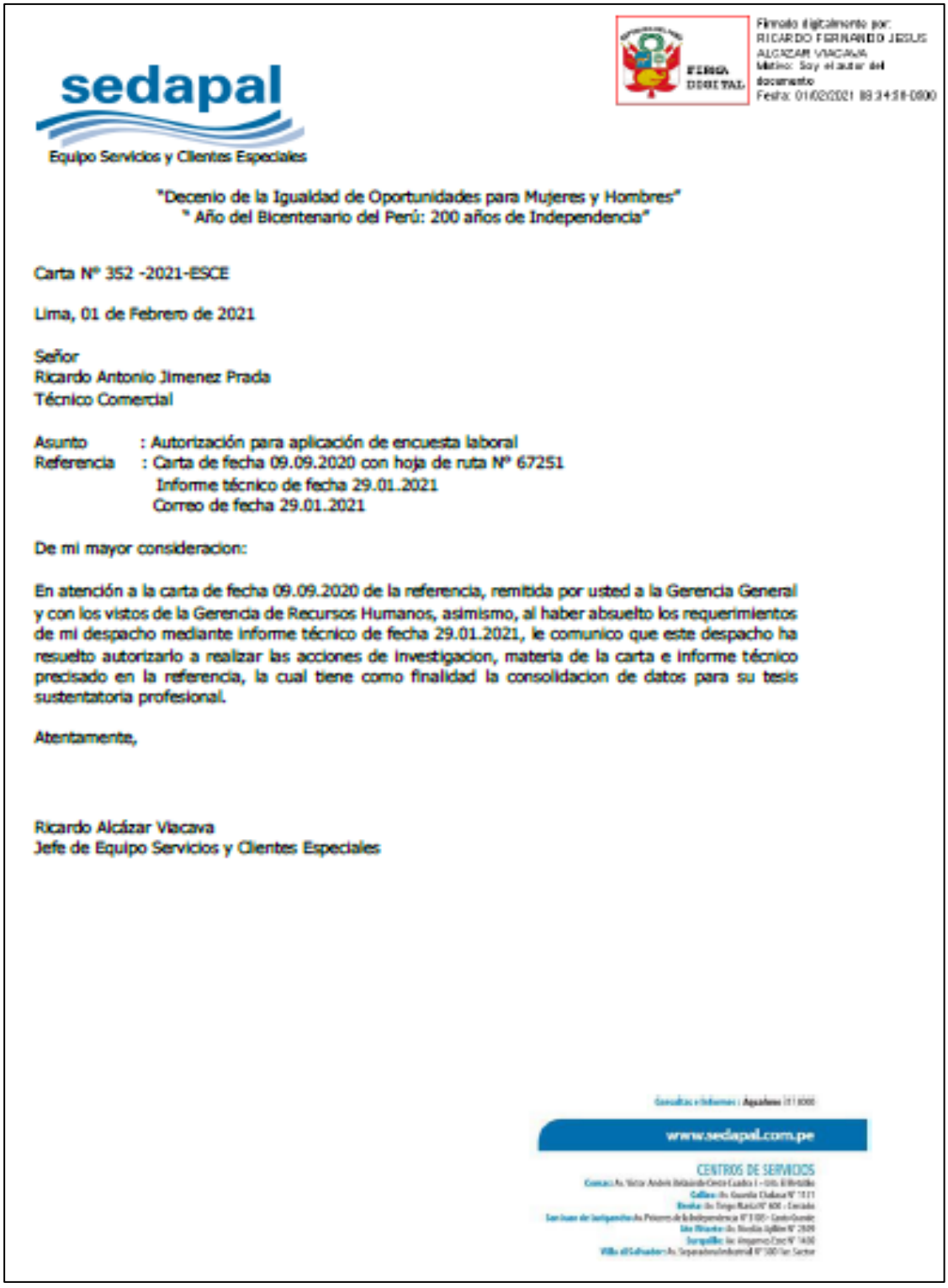
Atentamente

Ricardo Antonio Jiménez Prada
DNI 74607905

www.sedapal.com.pe

CENTROS DE SERVICIOS

Anexo 7: Carta de autorización de aplicación de encuesta.



sedapal

Equipo Servicios y Clientes Especiales

FIRMA DIGITAL

Firmado digitalmente por: RICARDO FERNANDO JESUS ALCAZAR VIACAVA
Motivo: Soy el autor del documento
Fecha: 01/02/2021 08:34:58-0800

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
" Año del Bicentenario del Perú: 200 años de Independencia"

Carta N° 352 -2021-ESCE

Lima, 01 de Febrero de 2021

Señor
Ricardo Antonio Jimenez Prada
Técnico Comercial

Asunto : Autorización para aplicación de encuesta laboral
Referencia : Carta de fecha 09.09.2020 con hoja de ruta N° 67251
Informe técnico de fecha 29.01.2021
Correo de fecha 29.01.2021

De mi mayor consideracion:

En atención a la carta de fecha 09.09.2020 de la referencia, remitida por usted a la Gerencia General y con los vistos de la Gerencia de Recursos Humanos, asimismo, al haber absuelto los requerimientos de mi despacho mediante informe técnico de fecha 29.01.2021, le comunico que este despacho ha resuelto autorizarlo a realizar las acciones de investigacion, materia de la carta e informe técnico precisado en la referencia, la cual tiene como finalidad la consolidacion de datos para su tesis sustentatoria profesional.

Atentamente,

Ricardo Alcázar Viacava
Jefe de Equipo Servicios y Clientes Especiales

www.sedapal.com.pe

CENTROS DE SERVICIOS

Anexo 8: Informe Técnico

Reconocimiento Biométrico por Huella Dactilar

La biometría es una tecnología de autenticación basada en el reconocimiento inequívoco de las propiedades únicas e intransferibles de un individuo.

De acuerdo con Serratosa (2012) explica que el reconocimiento biométrico se refiere al uso de diversas características anatómicas, los cuales se denominan identificadores biométricos que sirven para garantizar la identidad de un individuo (p. 14)

El reconocimiento biométrico en combinación con componentes sistematizados que proporciona una estructura de seguridad fortificada conducente a la autenticación univoca de individuos, debido a que esta no depende de factores que puedan ser extraviados o hurtados, sino que funciona como un mecanismo individual e intransferible propio de cada persona.

Los métodos tradicionales han sido eficaces, pero han representado una serie de inconvenientes, los cuales ponen en riesgo la información, asimismo, los conceptos que los representan, tales como la disponibilidad, integridad y confidencialidad. Por ello, que el reconocimiento por huella dactilar promueve en un sentido sustancial a la protección de estos recursos que están directa e indirectamente vulnerables a la mayor amenaza para la información, el fallo humano.

Según Das (2015) considera elementos que caracterizan las ventajas de esta tecnología, consolidando conceptos como universalidad, unicidad, permanencia, colectabilidad, rendimiento y aceptabilidad (pp. 59 - 62).

Marcel, Nixon y Li (2014) mencionan que, los rasgos biométricos siendo elementos únicos y fuertemente relacionados a un usuario en específico, pueden ser argumentados como seguros, ya que posea cierta ventaja sobre los demás, la cual permite verificar la identidad de un individuo de forma más confiable a comparación de los métodos tradicionales como contraseñas, que podrían ser comprometidas con un menor nivel de dificultad para diversos fines.

1. Metodología de desarrollo XP

La programación extrema o eXtreme Programming (XP) es una metodología de desarrollo de una ingeniera de software formulada por Kent Beck, autor del primer libro sobre la materia. Extreme Programming Explained: Embrace Chang (1999). Es el más destacado de los procesos agiles de desarrollo de software. Al igual que estos, la programación extrema se diferencia de las metodologías tradicionales principalmente en que pone más énfasis en la adaptabilidad que en la previsibilidad.

2. Justificación de selección de la metodología empleada

Respecto a la metodología ágil XP, destaca por su gran flexibilidad en cuanto a cambios y la reducción significativa para tiempos de desarrollo, se optó por este marco de trabajo debido a su gran similitud tanto con metodologías tradicionales, como ágiles, permitiendo evaluar integración de procedimientos.

A continuación, se describirá las ventajas cualitativas referidas al uso de la metodología XP:

- *Presupuesto*

El presupuesto es un punto clave a la hora de desarrollar un proyecto, es así que la metodología XP por ser una metodología ágil no demanda un elevado consumo de recursos y equipo de trabajo.

- *Tamaño del proyecto*

El enfoque de las metodologías tradicionales se orienta principalmente a proyectos de gran tamaño que involucran un desarrollo a largo plazo. La metodología XP tiene un enfoque hacia proyectos no muy prolongados.

- *Tiempos de entrega*

Un proyecto de desarrollo se encuentra limitado al tiempo, independientemente de su tamaño, la cual puede llevar a marcar un hito importante en la selección de la metodología a aplicarse. XP está diseñada para realizar entregas viables en tiempos relativamente cortos, debido a que se caracteriza por tener tiempos cortos de diseño, desarrollo e iteraciones.

- *Documentación*

La organización documentaria no resulta ser un requisito indispensable para los diferentes equipos de trabajo, debido a que no todas las organizaciones requieren manejar documentación detallada en relación a sus procesos y software utilizados. Por dicho motivo, la creación de manuales de usuario en las organizaciones es un aspecto netamente opcional, por lo que en este sentido se optó por utilizar la metodología desarrollo ágil XP al carecer del manejo de una documentación formal para el desarrollo de los proyectos, la única documentación que esta metodología ofrece es el código resultado de las diferentes iteraciones.

- *Equipo de trabajo*

El número de requerimientos (personas, habilidades y competencias) y recursos necesarios (hardware y software) se encuentran estrechamente relacionado al tamaño de cada proyecto, he aquí la razón de contar con un equipo interdisciplinario y coordinado. XP posee una serie de roles dentro del equipo de trabajo para el control de procesos, e iteraciones como también consideraciones de flexibilidad en el número de miembros del equipo, el cual no debería sobrepasar el total de 15 personas.

- *Adaptabilidad*

La posibilidad de que ocurra un cambio repentino varía de acuerdo al tipo de proyecto. Esta metodología se orienta a la flexibilidad que posee en respuesta a los cambios que pueden aparecer durante el desarrollo del mismo.

- *Disponibilidad del cliente*

Una de las partes importantes durante el desarrollo de la metodología, es aquel relacionado con los requerimientos y especificaciones del proyecto de software, por tanto, la valorización de quien provee la información, asimismo, de la disponibilidad de tiempo para el proyecto es un tema a tomar en consideración. Al respecto, XP como parte de su estructura de desarrollo posee como principio fundamental la participación del cliente de una forma inclusiva e integradora con el equipo de trabajo, orientada al éxito del proyecto.

3. Fases de la Metodología XP

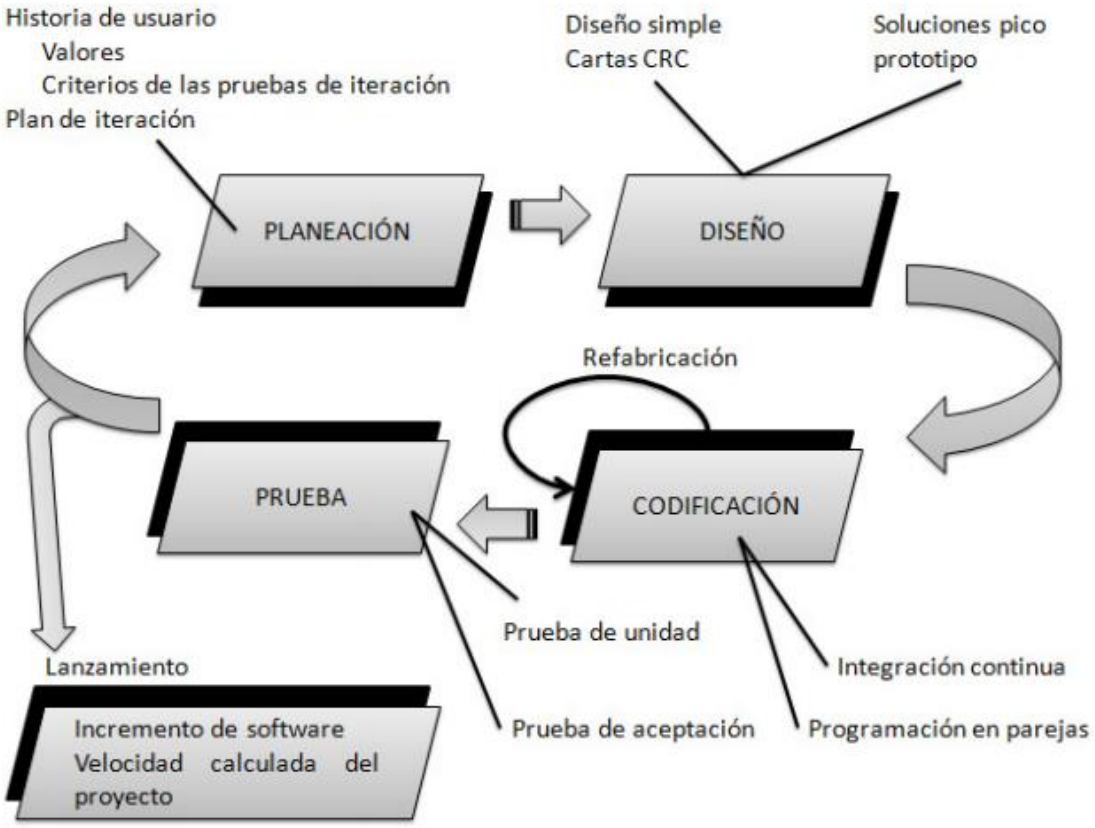


Figura 1. Etapas del Desarrollo de XP (Pressman, 2010)

Planeación

Esta primera fase se orienta en entender los requerimientos y contexto del negocio a través de las experiencias del cliente con el objetivo de identificar las funcionalidades y características (Pressman, 2010, p. 62).

Estas características se obtienen por medio de historias de usuario, las cuales resultan de las coordinaciones del grupo de trabajo y el cliente (Wells, 1999). Habiendo realizado las historias de trabajo, se divide las tareas entre el equipo de trabajo, los recursos a utilizar, se genera un cronograma de entregas y las iteraciones (Sommerville, 2005).

Diseño

Kendall & Kendall (2005) definen como la fase de evaluación para dividir las tareas conformadas en base a cada historia de usuario, cada tarea representa una característica exclusiva del sistema, la cual se puede diseñar individualmente en virtud de una integración colectiva.

Desarrollo

Se procede a la programación unitaria y a la integración del código de acuerdo a una jerarquía de dependencias (Kendall & Kendall, 2005).

En esta etapa se espera una retroalimentación por medio de la cooperación con el usuario, en la medida de satisfacer las necesidades y mejoras para el proyecto.

Pruebas

De acuerdo a las características individuales del sistema cada una de ellas con una funcionalidad (historias de usuario) especifica, es sometida a pruebas unitarias, las cuales están diseñadas para evaluar los métodos y clases por los programadores y testers (Sommerville, 2005).

4. Sistema de reconocimiento biométrico por huella dactilar

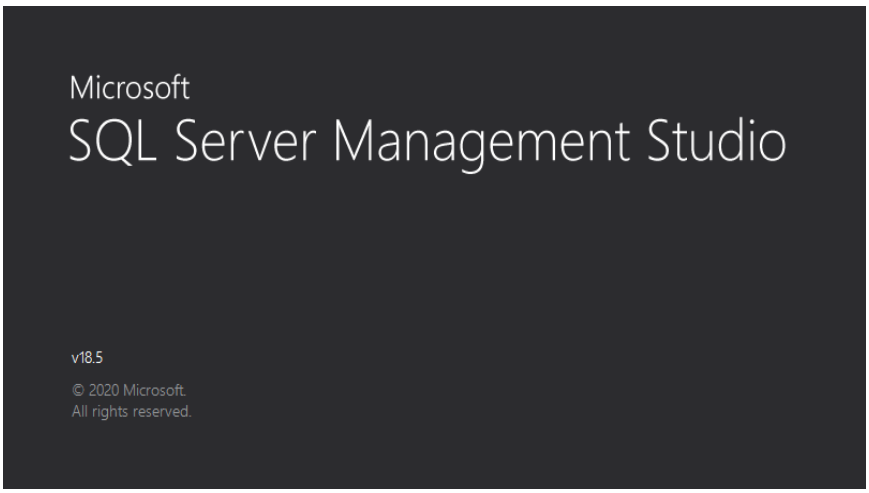


Figura 2. Sistema de Gestión de base de datos SQL Server Managment Studio

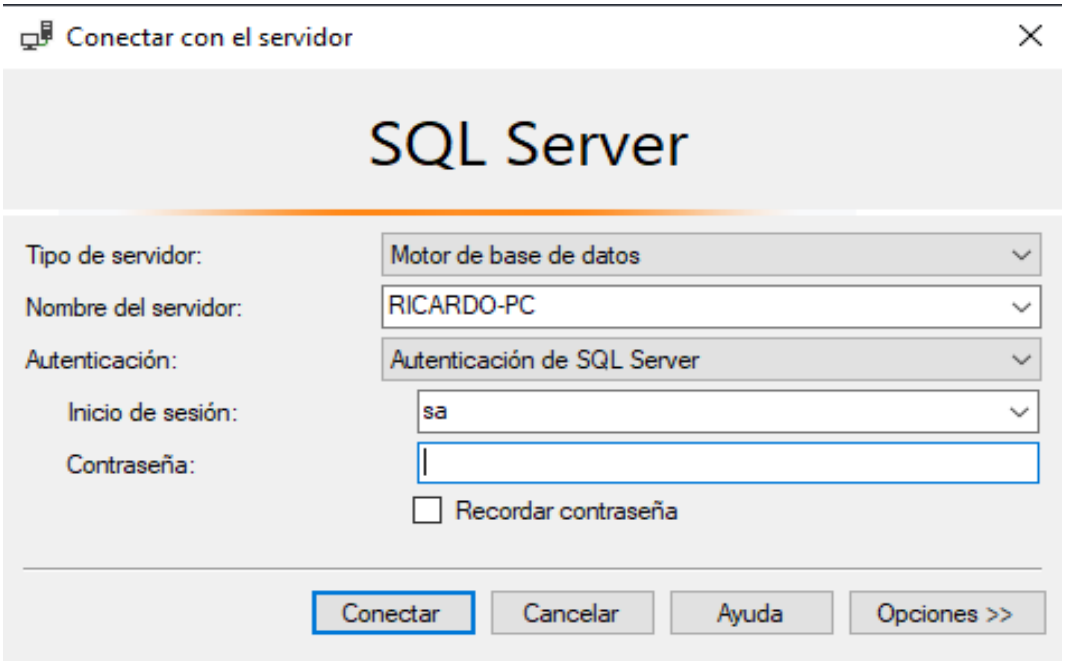


Figura 3. Motor de base de datos SQL Server

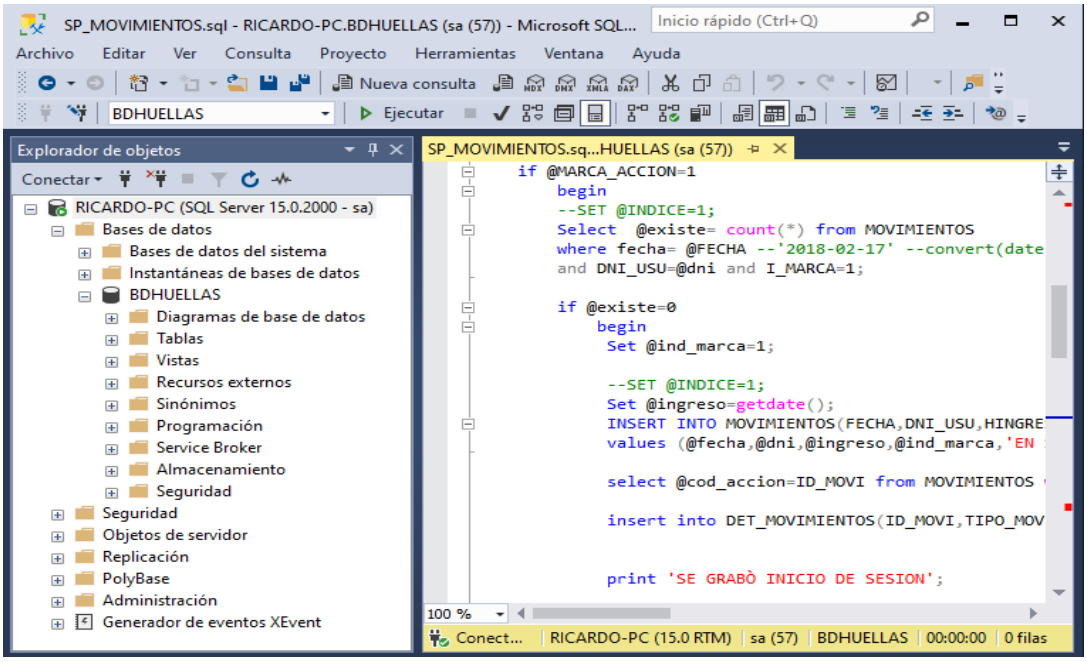


Figura 4. Interfaz gráfica del sistema del sistema de gestión de base de datos SQL Server Managment Studio 2016

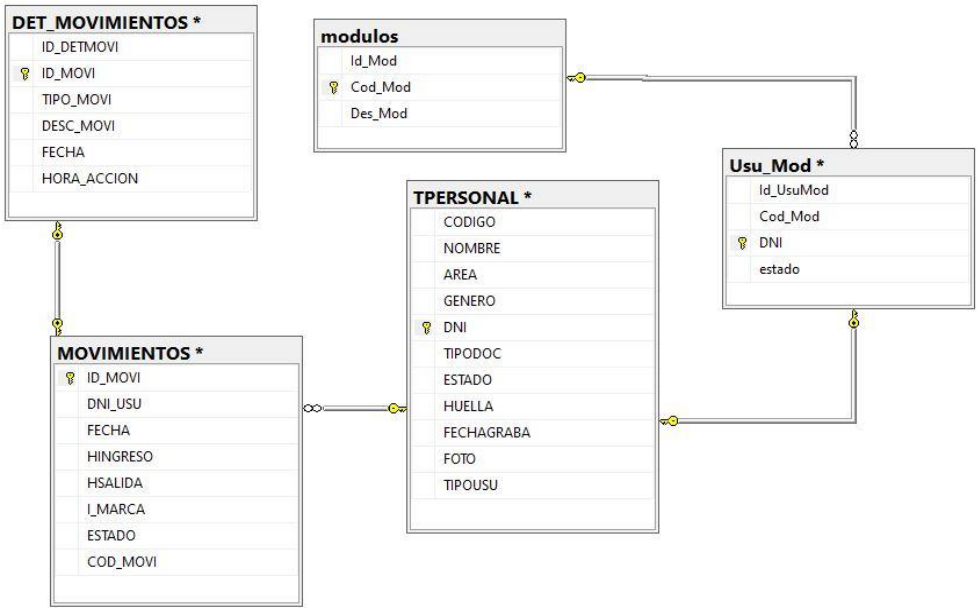


Figura 5. Diagrama de la base de datos BDHUELLAS.

RICARDO-PC.BDH...DET_MOVIMIENTOS

Nombre de columna	Tipo de datos
ID_DETMOVI	int
ID_MOVI	int
TIPO_MOVI	varchar(100)
DESC_MOVI	varchar(300)
FECHA	date
HORA_ACCION	datetime

RICARDO-PC.BDHU...AS - dbo.modulos

Nombre de columna	Tipo de datos
Id_Mod	int
Cod_Mod	char(10)
Des_Mod	varchar(50)

RICARDO-PC.BDHU...- dbo.TPERSONAL

Nombre de columna	Tipo de datos
CODIGO	int
NOMBRE	nchar(50)
AREA	nchar(50)
GENERO	nchar(30)
DNI	nchar(12)
TIPODOC	nchar(50)
ESTADO	nchar(50)
HUELLA	image
FECHAGRABA	datetime
FOTO	image
TIPOUSU	char(1)

RICARDO-PC.BDH...dbo.MOVIMIENTOS

Nombre de columna	Tipo de datos
ID_MOVI	int
DNI_USU	nchar(12)
FECHA	date
HINGRESO	datetime
HSALIDA	datetime
I_MARCA	int
ESTADO	varchar(50)
COD_MOVI	int

RICARDO-PC.BDHU...AS - dbo.Usu_Mod

Nombre de columna	Tipo de datos
Id_UsuMod	int
Cod_Mod	char(10)
DNI	nchar(12)
estado	int

Figura 6. Diseño de tablas de la base de datos BDHUELLAS.

```
CREATE PROCEDURE SP_MOVIMIENTOS (
@FECHA DATE,
@DNI VARCHAR(12),
@MARCA_ACCION INT,
@DESCRIPCION VARCHAR(200),
@ACCION VARCHAR(100))

AS
BEGIN
	declare @existe int ;
	declare @existe2 int ;
	declare @ingreso datetime;
	declare @ind_marca int;
	declare @cod_accion int;
	declare @lee_marca int;
	declare @marcas int;
	declare @contadormarcas int
	declare @contadormarcas2 int


if @MARCA_ACCION=1 -- SI ES ACCESO
begin

Select  @existe2= count(*) from MOVIMIENTOS -- numero de sesiones con ese usuario
	where DNI_USU=@dni

Select @existe= count (*) from MOVIMIENTOS -- si existe alguna sesión
con ese usuario y la fecha actual
where fecha= @FECHA --'2018-02-17' --convert(date,getdate())
and DNI_USU=@dni and I_MARCA=1;

if @existe2=0 -- si no existe alguna sesion con ese usuario
BEGIN
	Set @ind_marca=1;-- 1 es en sesion y 2 es sesion cerrada
	Set @ingreso=getdate();-- hora y fecha que inicio la sesion
	INSERT INTO MOVIMIENTOS(FECHA,DNI_USU,HINGRESO,I_MARCA,ESTADO,COD_MOVI)
	values (@fecha,@dni,@ingreso,@ind_marca,'EN SESION',1) ;

select @cod_accion=ID_MOVI from MOVIMIENTOS where DNI_USU=@dni and I_MARCA=1;

insert into DET_MOVIMIENTOS(ID_MOVI,TIPO_MOVI,DESC_MOVI,FECHA,HORA_ACCION) values
(@cod_accion,@ACCION,@DESCRIPCION,@FECHA,@ingreso);
print 'SE GRABÒ INICIO DE SESION POR PRIMERA VEZ';
END
	ELSE -- si existe alguna sesion con ese usuario
	BEGIN
	SELECT @marcas=count(*) FROM MOVIMIENTOS WHERE DNI_USU=@dni and I_MARCA=1;
	if @marcas=1-- si el usuario tiene una sesion abierta
	begin
	-- if que indica si es cierre de sesion o si encontró una sesion abierta

	if @DESCRIPCION='SESION CERRADA' --indica que la sesion actual esta siendo cerrada
	begin
	-- SE CIERRA LA SESION ABIERTA

	Set @ingreso=getdate();
	select @cod_accion=ID_MOVI from MOVIMIENTOS where DNI_USU=@dni and I_MARCA=1;

insert into DET_MOVIMIENTOS(ID_MOVI,TIPO_MOVI,DESC_MOVI,FECHA,HORA_ACCION) values (@cod_accion,@ACCION,'SESION
CERRADA',@FECHA,@ingreso);

Update MOVIMIENTOS set HSALIDA=getdate(), I_MARCA=2, ESTADO='SESION CERRADA' where  DNI_USU=@dni and I_MARCA=1;
print 'SE MARCO CIERRE DE SESION';
end
else -- indica si al iniciar sesion encuentra una sesion anterior abierta
begin

-- SE CIERRA LA SESION ABIERTA
Set @ingreso=getdate();
select @cod_accion=ID_MOVI from MOVIMIENTOS where DNI_USU=@dni and I_MARCA=1;

insert into DET_MOVIMIENTOS(ID_MOVI,TIPO_MOVI,DESC_MOVI,FECHA,HORA_ACCION) values (@cod_accion,@ACCION,'SESION
CERRADA',@FECHA,@ingreso);

Update MOVIMIENTOS set HSALIDA=getdate(), I_MARCA=2, ESTADO='SESION CERRADA' where  DNI_USU=@dni and I_MARCA=1;
print 'SE MARCO CIERRE DE SESION';

-- SE MARCA INGRESO
select top (1)@contadormarcas=COD_MOVI from MOVIMIENTOS WHERE DNI_USU=@dni and I_MARCA=2 ORDER BY HINGRESO DESC;
```

```
set @contadormarcas2=@contadormarcas+1;
Set @ind_marca=1;
Set @ingreso=getdate();
INSERT INTO MOVIMIENTOS(FECHA,DNI_USU,HINGRESO,I_MARCA,ESTADO,COD_MOVI)
values (@fecha,@dni,@ingreso,@ind_marca,'EN SESION',@contadormarcas2);

select @cod_accion=ID_MOVI from MOVIMIENTOS where DNI_USU=@dni and I_MARCA=1;
insert into DET_MOVIMIENTOS(ID_MOVI,TIPO_MOVI,DESC_MOVI,FECHA,HORA_ACCION) values
(@cod_accion,@ACCION,@DESCRIPCION,@FECHA,@ingreso);
print 'SE GRABÒ INICIO DE SESION';
      end
      end

else
begin
select top (1)@contadormarcas=COD_MOVI from MOVIMIENTOS WHERE DNI_USU=@dni ORDER BY HINGRESO DESC;
set @contadormarcas2=@contadormarcas+1;
Set @ind_marca=1;
Set @ingreso=getdate();
INSERT INTO MOVIMIENTOS(FECHA,DNI_USU,HINGRESO,I_MARCA,ESTADO,COD_MOVI)
values (@fecha,@dni,@ingreso,@ind_marca,'EN SESION',@contadormarcas2);

select @cod_accion=ID_MOVI from MOVIMIENTOS where DNI_USU=@dni and I_MARCA=1;
insert into DET_MOVIMIENTOS(ID_MOVI,TIPO_MOVI,DESC_MOVI,FECHA,HORA_ACCION) values
(@cod_accion,@ACCION,@DESCRIPCION,@FECHA,@ingreso);
print 'SE GRABÒ INICIO DE SESION';
end
END

end

ELSE IF @MARCA_ACCION=2 -- si es actualizacion
      BEGIN
      Set @ingreso=getdate();
      select @cod_accion=ID_MOVI from MOVIMIENTOS where DNI_USU=@dni and FECHA=@FECHA and I_MARCA=1;

      insert into DET_MOVIMIENTOS(ID_MOVI,TIPO_MOVI,DESC_MOVI,FECHA,HORA_ACCION) values
(@cod_accion,@ACCION,@DESCRIPCION,@FECHA,@ingreso);


       END

ELSE
      BEGIN
      PRINT 'NO HAY INSTRUCCIONES PARA ESTE TIPO DE ACCION';

END

RETURN
END
```

Figura 7. Procedimiento almacenado de control de sesiones.

Figura 8. Herramienta de desarrollo Visual Studio 2019.

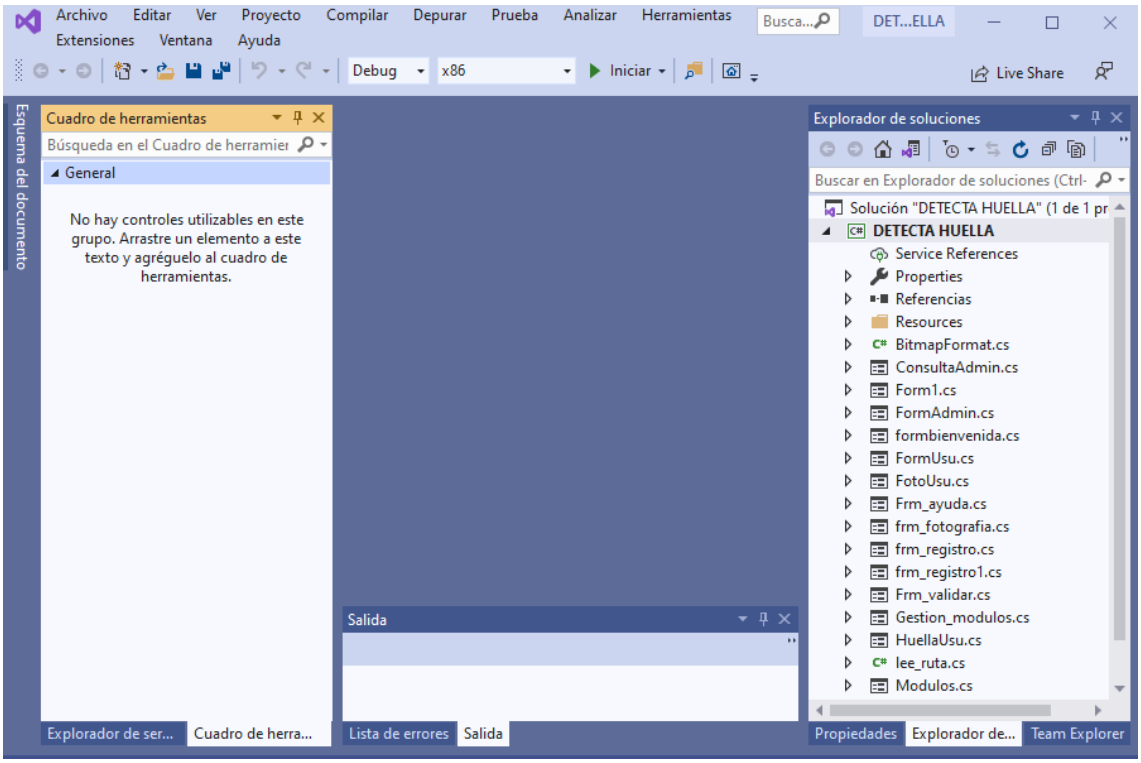


Figura 9. Entorno de desarrollo integrado Visual Studio 2019.

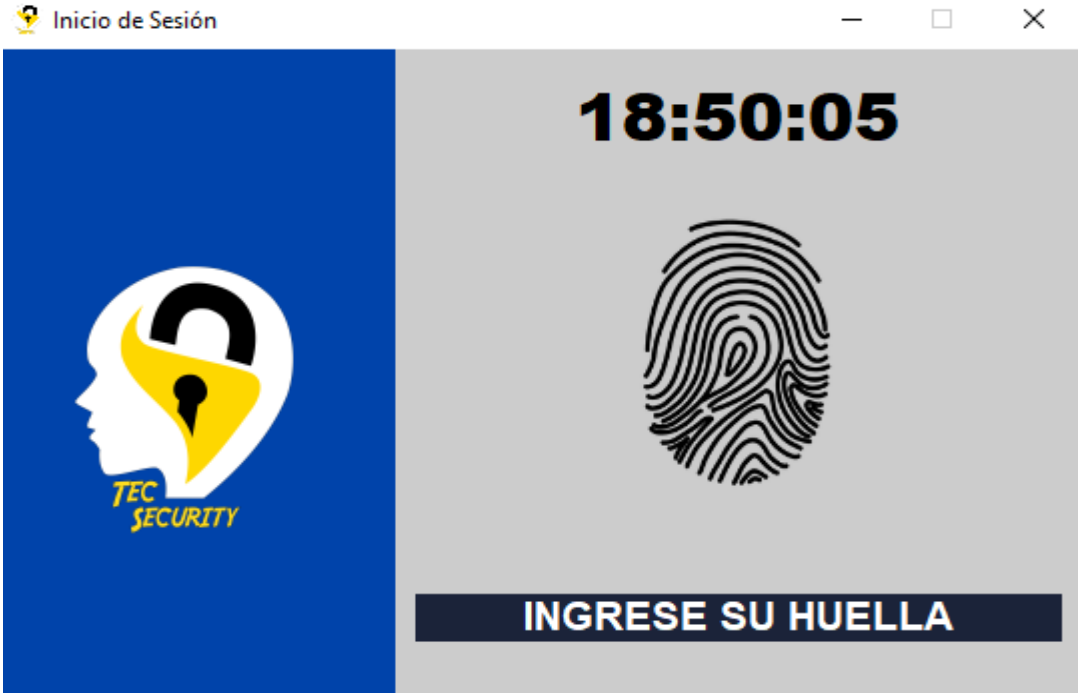


Figura 10. Módulo de inicio de sesión.

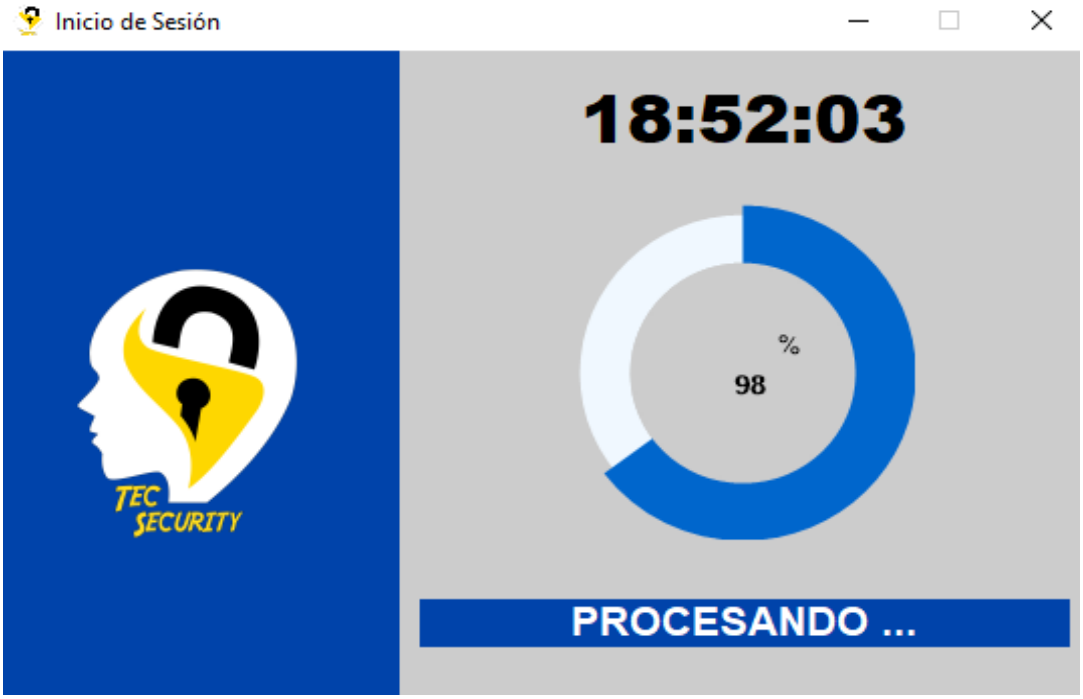


Figura 11. Módulo de inicio de sesión procesando huella dactilar.

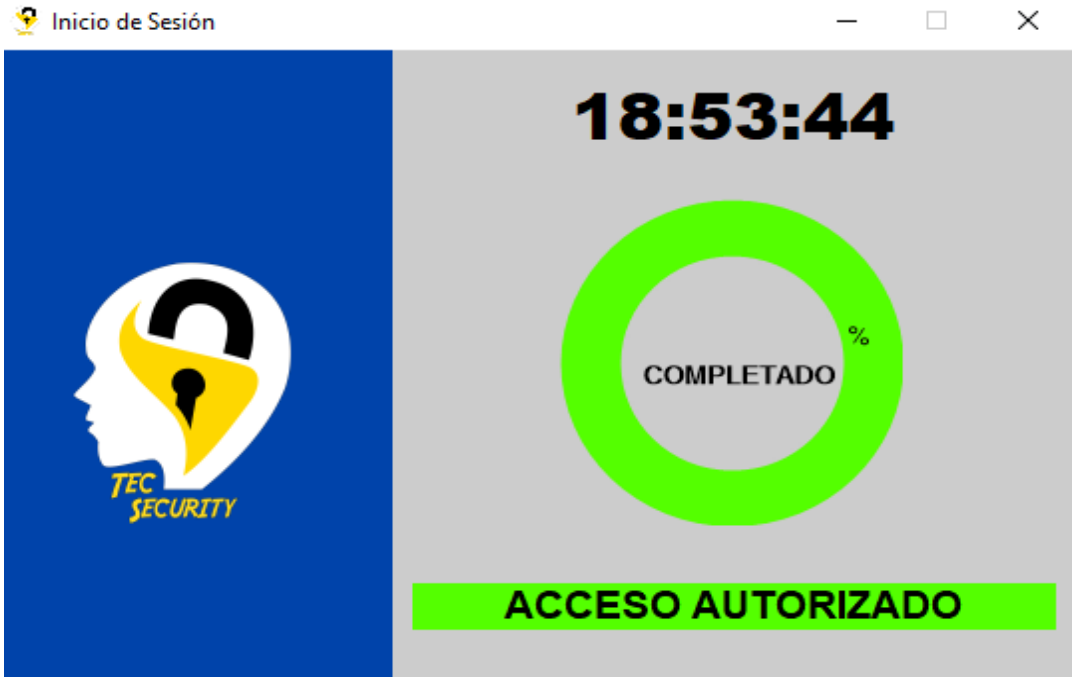


Figura 12. Módulo de inicio de sesión autorizando acceso.

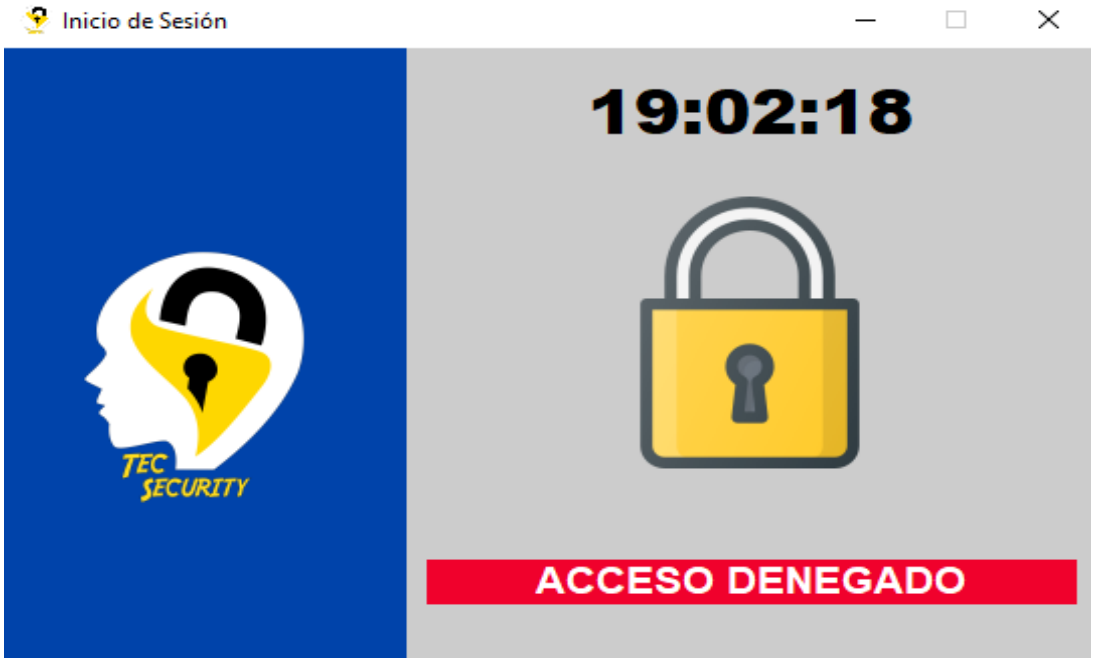


Figura 13. Módulo de inicio de sesión acceso denegado.

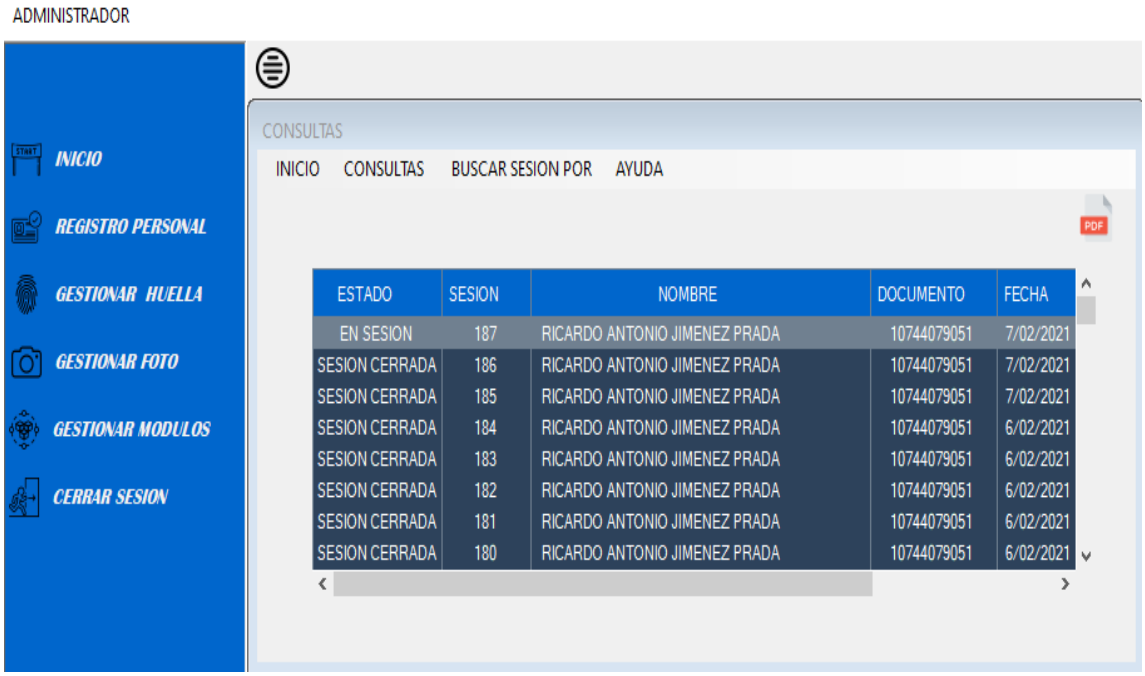


Figura 14. Ventana principal.

Figura 15. Módulo de registro de personal.

Figura 16. Módulo de registro y actualización de huella dactilar.

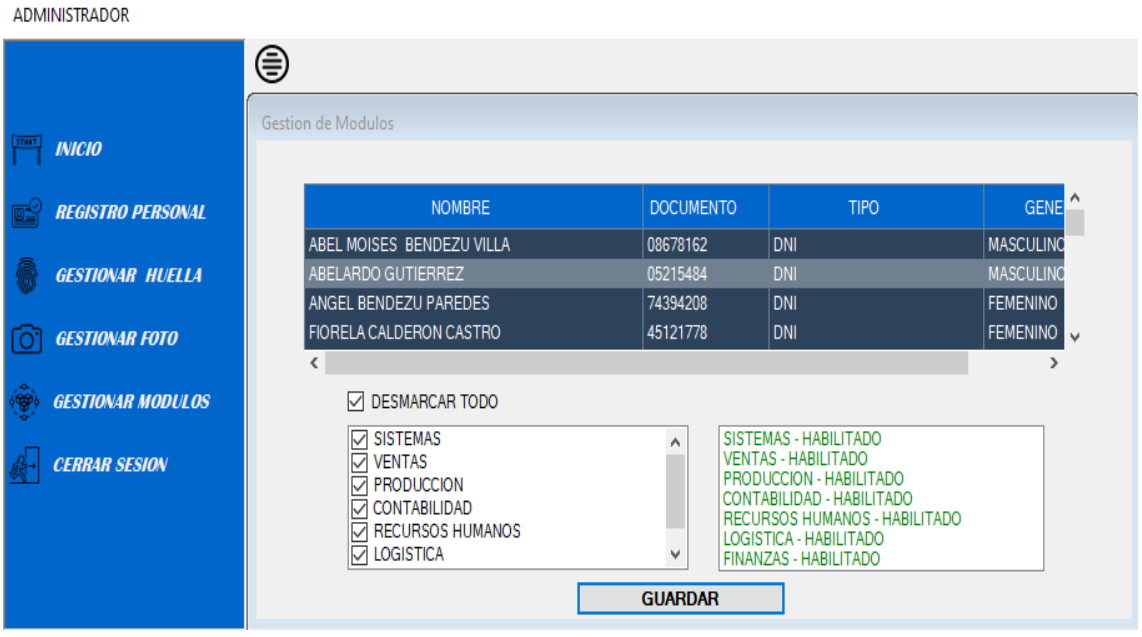


Figura 17. Módulo de asignación de áreas.

Figura 18. Módulo de registro y actualización de foto.

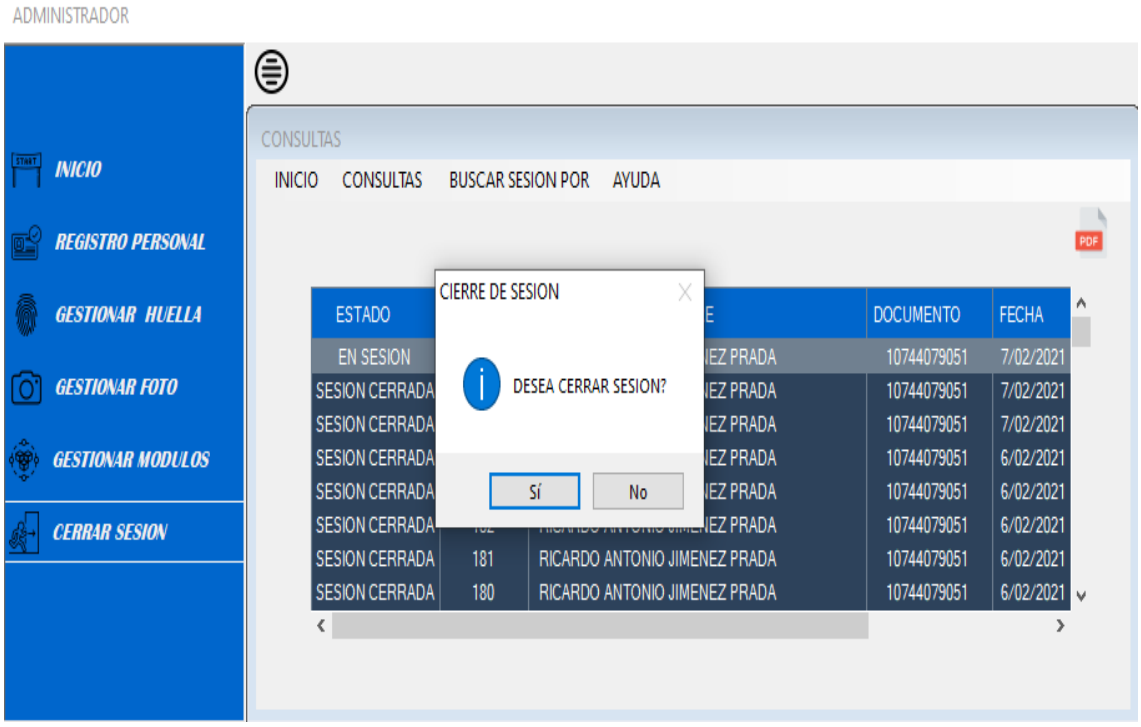


Figura 19. Módulo de cierre de sesión.

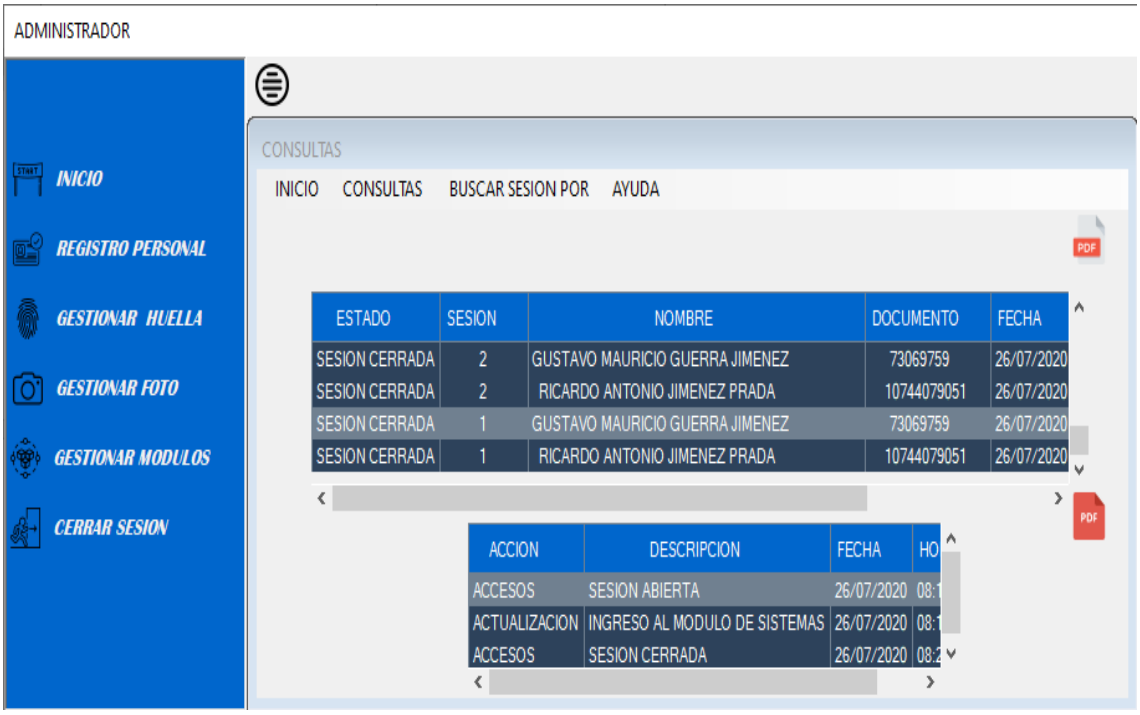


Figura 20. Módulo central con detalle de sesiones.

Figura 21. Módulo de consultas generales.

Figura 22. Módulo de consultas especificas por criterio búsqueda (por fecha).

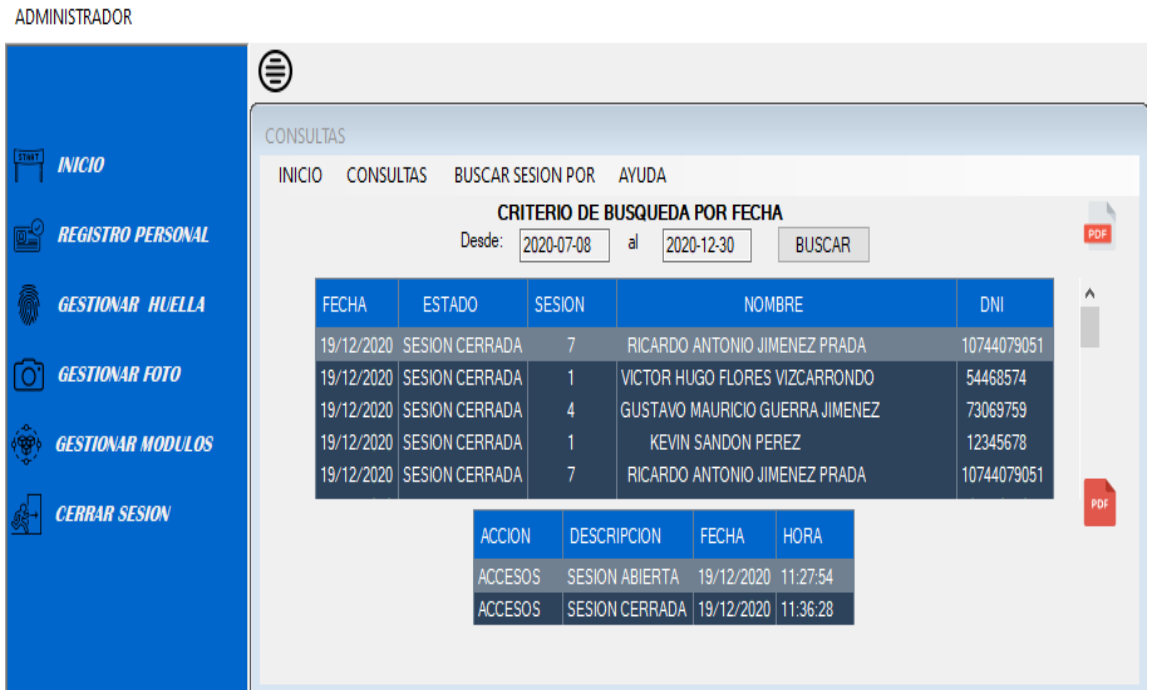
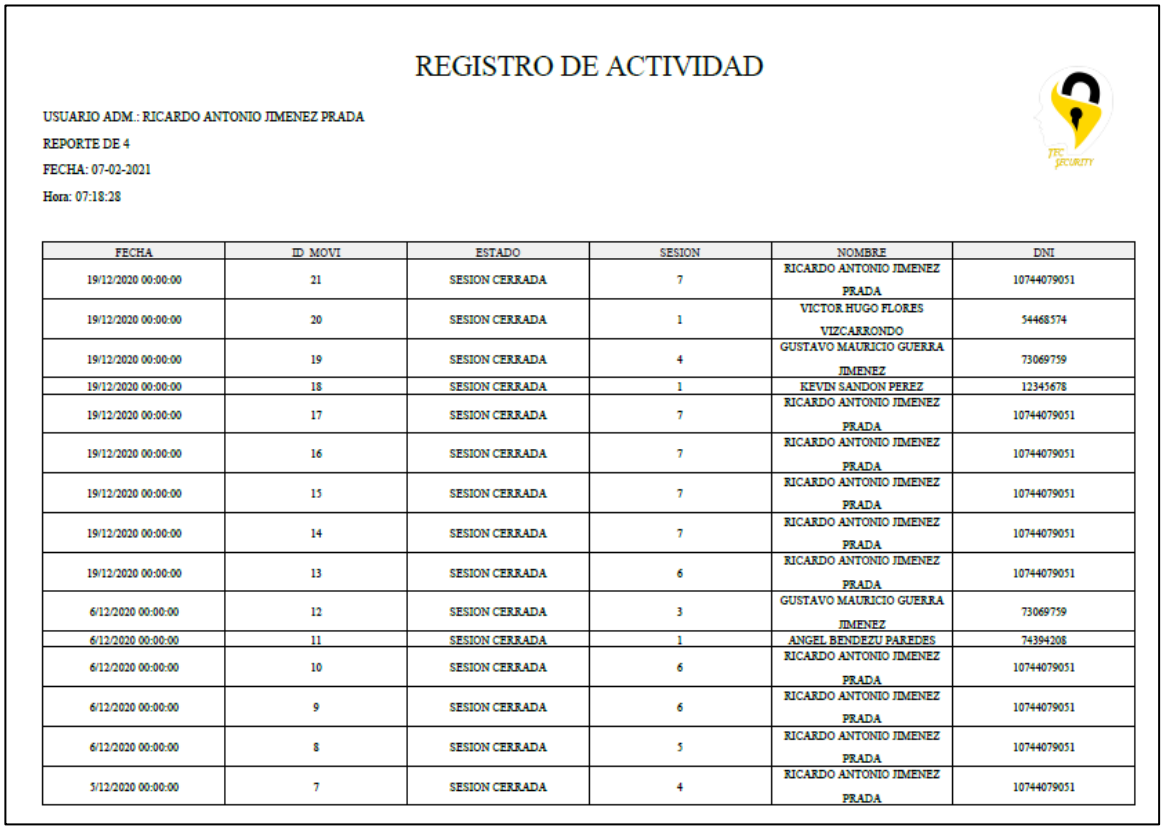


Figura 23. Módulo de consultas especificas por criterio búsqueda (por rango de fechas).

Figura 24. Módulo de ayuda informativa.

Figura 25. Módulo de previo de generación de reportes.



REGISTRO DE ACTIVIDAD

USUARIO ADM.: RICARDO ANTONIO JIMENEZ PRADA

REPORTE DE 4

FECHA: 07-02-2021

Hora: 07:18:28

FECHA	ID_MOVI	ESTADO	SESION	NOMBRE	DNI
19/12/2020 00:00:00	21	SESION CERRADA	7	RICARDO ANTONIO JIMENEZ PRADA	10744079051
19/12/2020 00:00:00	20	SESION CERRADA	1	VICTOR HUGO FLORES VIZCARRONDO	54468574
19/12/2020 00:00:00	19	SESION CERRADA	4	GUSTAVO MAURICIO GUERRA JIMENEZ	73069759
19/12/2020 00:00:00	18	SESION CERRADA	1	KEVIN SANDON PEREZ	12345678
19/12/2020 00:00:00	17	SESION CERRADA	7	RICARDO ANTONIO JIMENEZ PRADA	10744079051
19/12/2020 00:00:00	16	SESION CERRADA	7	RICARDO ANTONIO JIMENEZ PRADA	10744079051
19/12/2020 00:00:00	15	SESION CERRADA	7	RICARDO ANTONIO JIMENEZ PRADA	10744079051
19/12/2020 00:00:00	14	SESION CERRADA	7	RICARDO ANTONIO JIMENEZ PRADA	10744079051
19/12/2020 00:00:00	13	SESION CERRADA	6	RICARDO ANTONIO JIMENEZ PRADA	10744079051
6/12/2020 00:00:00	12	SESION CERRADA	3	GUSTAVO MAURICIO GUERRA JIMENEZ	73069759
6/12/2020 00:00:00	11	SESION CERRADA	1	ANGEL BENDEZU PAREDES	74394208
6/12/2020 00:00:00	10	SESION CERRADA	6	RICARDO ANTONIO JIMENEZ PRADA	10744079051
6/12/2020 00:00:00	9	SESION CERRADA	6	RICARDO ANTONIO JIMENEZ PRADA	10744079051
6/12/2020 00:00:00	8	SESION CERRADA	5	RICARDO ANTONIO JIMENEZ PRADA	10744079051
5/12/2020 00:00:00	7	SESION CERRADA	4	RICARDO ANTONIO JIMENEZ PRADA	10744079051

Figura 26. Reporte de sesiones general.

REGISTRO DE ACTIVIDAD

USUARIO ADM.: RICARDO ANTONIO JIMENEZ PRADA

REPORTE DE 10744079051

FECHA: 07-02-2021

Hora: 07:23:04

ESTADO	SESION	NOMBRE	DOCUMENTO	FECHA	HORA INGRESO	HORA SALIDA
SESION CERRADA	4	GUSTAVO MAURICIO GUERRA JIMENEZ	73069759	19/12/2020 00:00:00	11:21:20	11:21:28
SESION CERRADA	3	GUSTAVO MAURICIO GUERRA JIMENEZ	73069759	6/12/2020 00:00:00	07:20:34	07:20:52
SESION CERRADA	2	GUSTAVO MAURICIO GUERRA JIMENEZ	73069759	26/07/2020 00:00:00	08:33:35	08:42:38
SESION CERRADA	1	GUSTAVO MAURICIO GUERRA JIMENEZ	73069759	26/07/2020 00:00:00	08:19:39	08:20:34

Figura 27. Reporte de sesiones especifica.

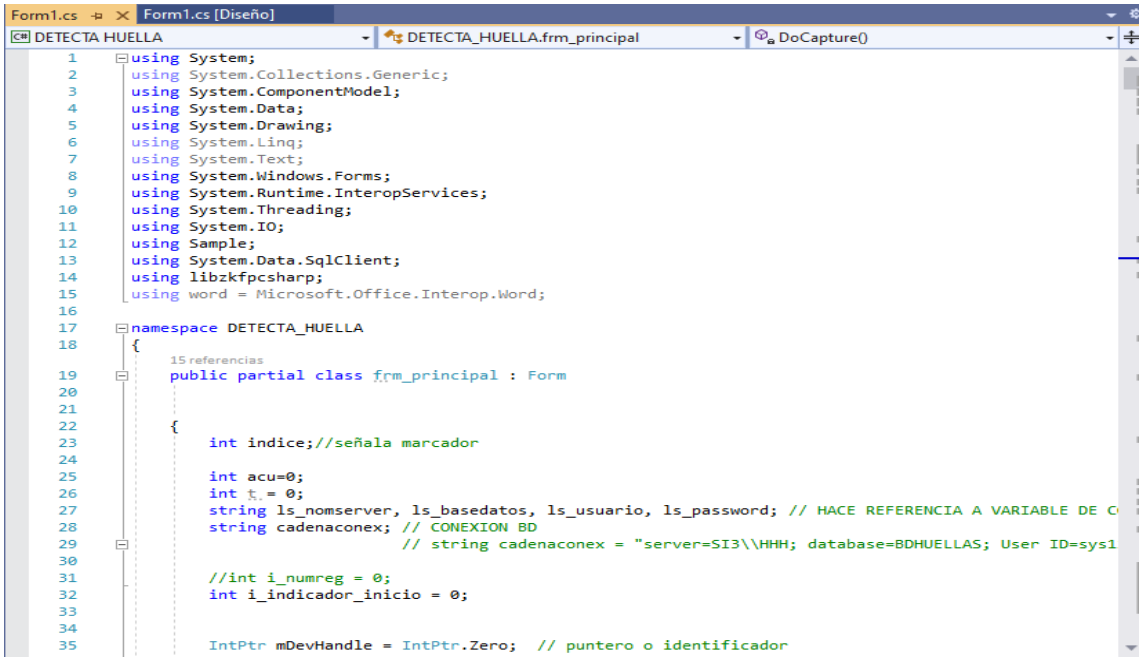


Figura 28. Código Fuente 01

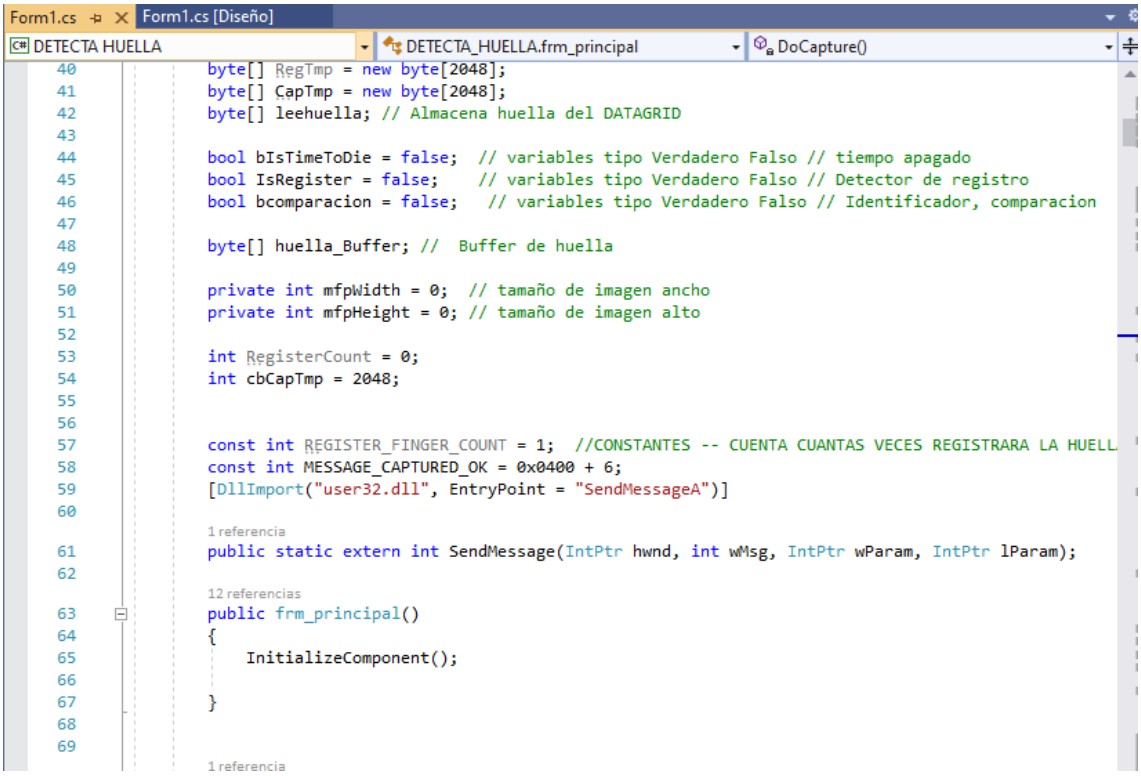


Figura 29. Código Fuente 02.

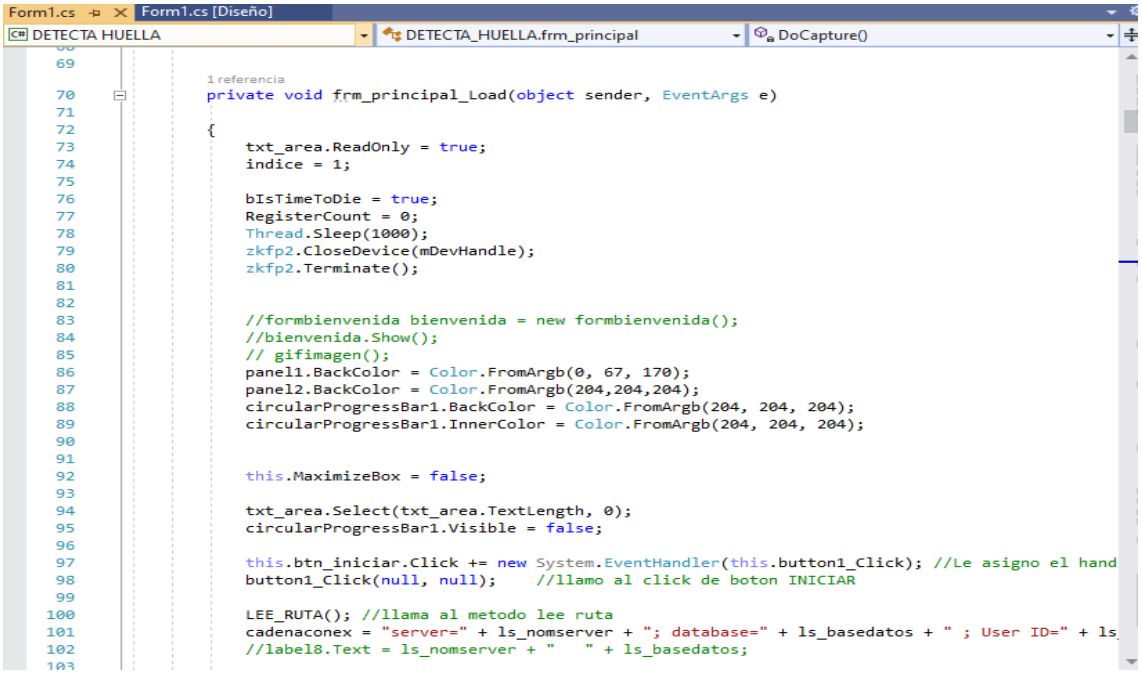


Figura 30. Código Fuente 03.

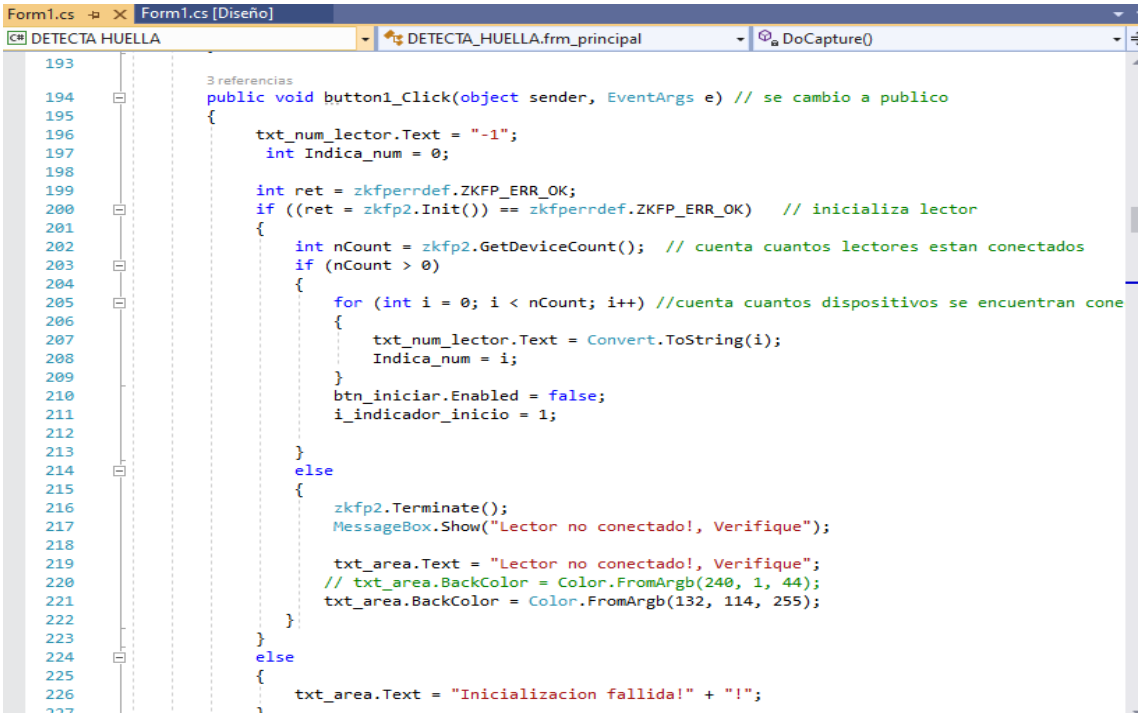


Figura 31. Código Fuente 04.

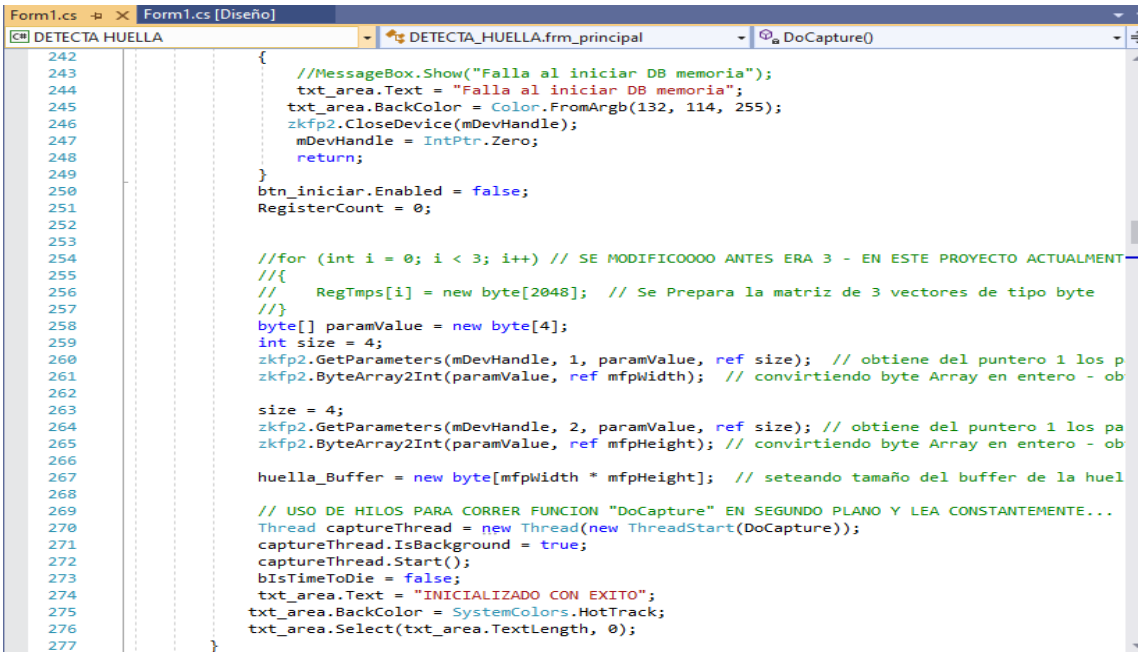


Figura 32. Código Fuente 05.

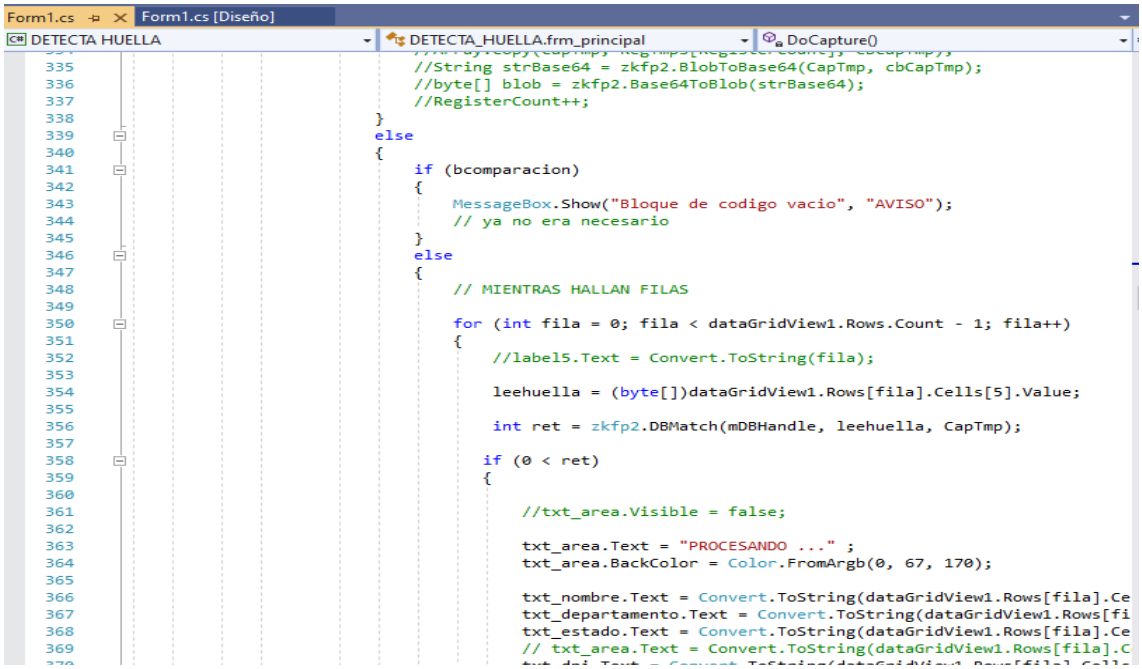


Figura 33. Código Fuente 06.

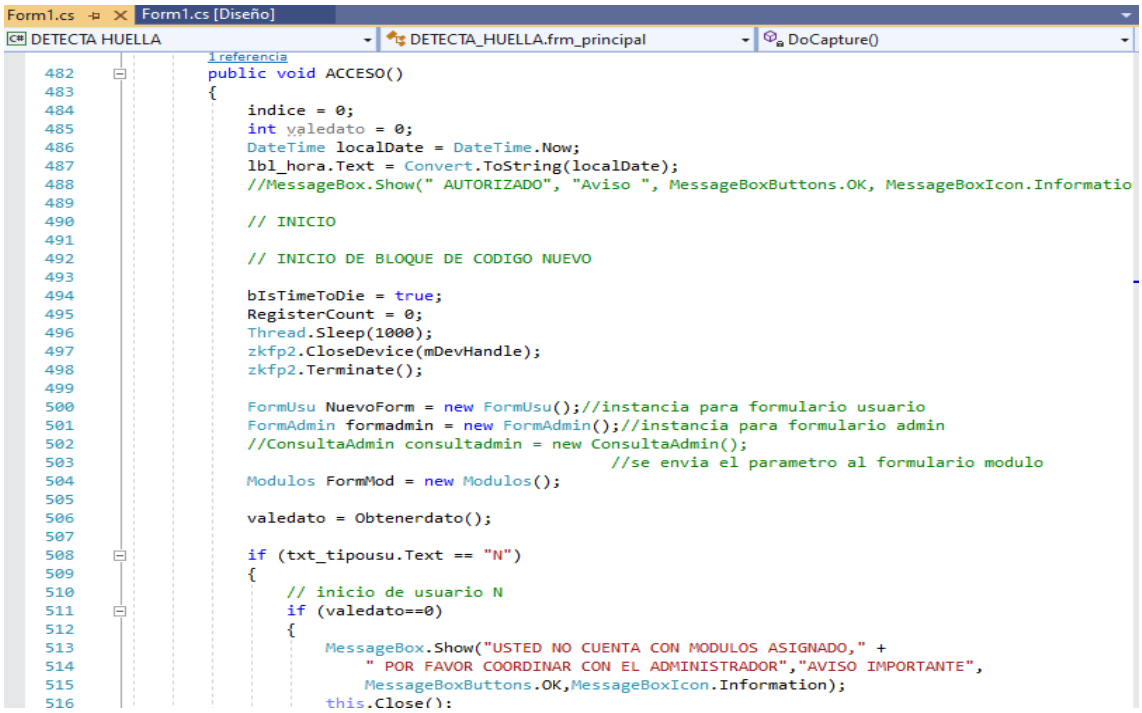


Figura 34. Código Fuente 07.

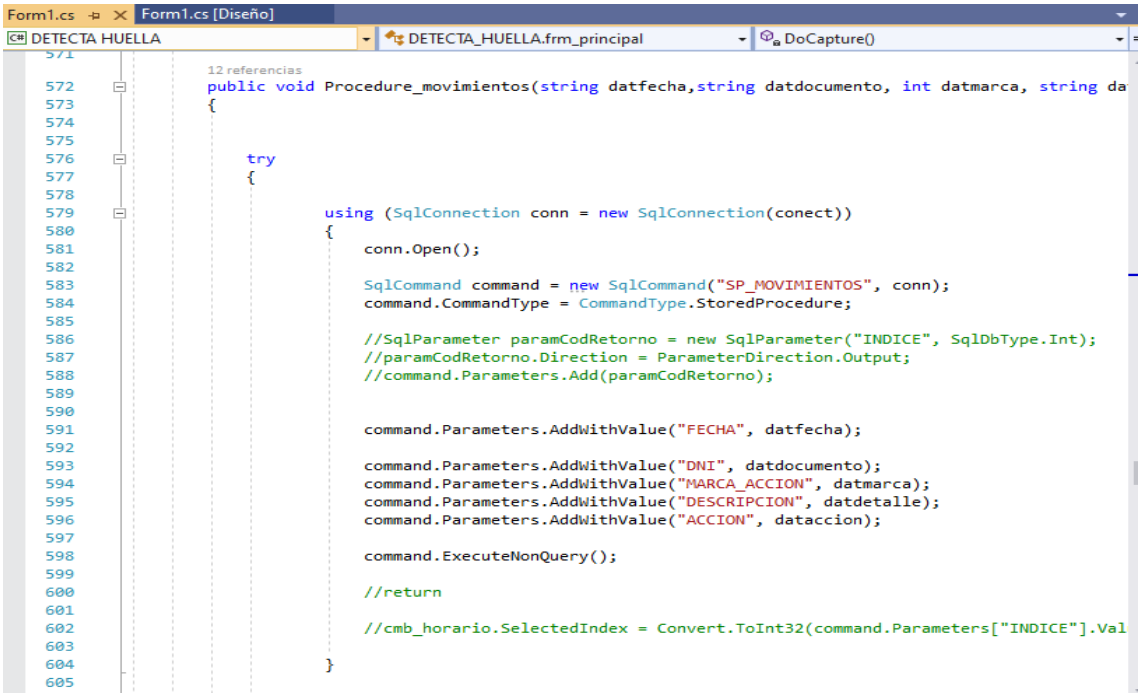


Figura 35. Código Fuente 08.

5. Lector Biométrico de Huella Dactilar ZKTECO ZK-4500

Descripción:

- Es un lector de huellas digitales diseñado para labores de integración con programas de aplicación. Mediante este lector es posible realizar las siguientes labores:

- Obtener las imágenes (archivos BPM o JPG) de la huella digital.

- Capturar un archivo con características que han única a la huella digital para realizar posteriores labores de verificación y/o identificación mediante la comparación de una huella viva colocada en el lector y huellas almacenadas en una base de datos.

Características:

- Alto rendimiento.

- Sensor óptico de huellas dactilares sin necesidades de mantenimiento.

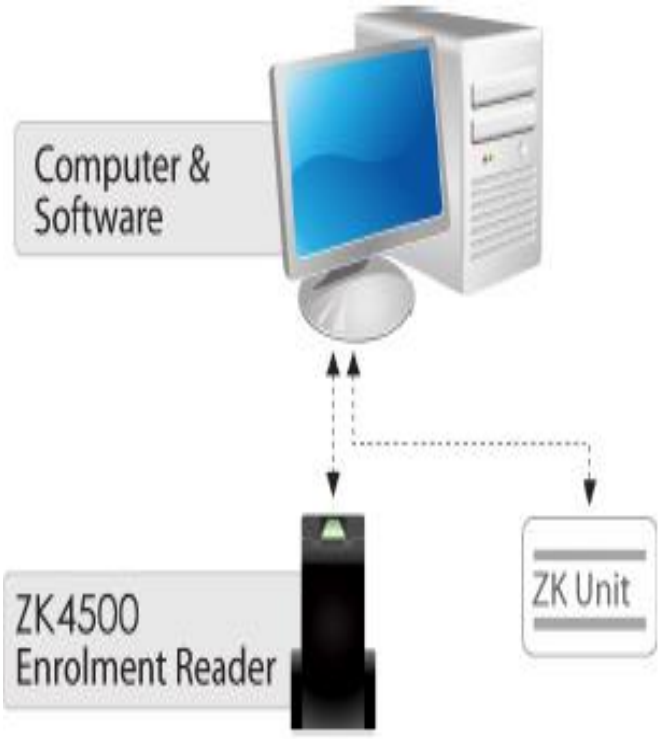
- De fácil acceso para cualquier dedo.

- Alta calidad de clase industrial de plástico ABS material con textura de la superficie resistente al rayado.

- Soporte extraíble.

- Interfaz USB de alta velocidad.

- LED indica estado del dispositivo.



Especificaciones:

- Sensor de huellas dactilares: Óptico
- Resolución: 500 DPI / 256 gris
- Detección de área: 15 * 18 mm
- Tamaño de imagen: 280 * 360 px
- Interfaz USB
- Apoyo O / S: Windows XP y Vista, Windows 7
- Color: Negro
- Dimensiones (WxLxH): 65,5 mm * 49 mm * 79.8 mm.

6. Factibilidad económica

Tabla N° 1. Materiales e insumos

DESCRIPCION	CANTIDAD	UNIDAD (S/)	TOTAL (S/)
Impresiones	06	14	S/ 84.00
Copias	50	0.10	S/ 5.00
Anillados	06	2.50	S/ 15.00
Fichas Bibliograficas	03	3.50	S/ 10.50
Utiles de Oficina	02	12.00	S/ 24.00
Pasajes	54	5.00	S/ 270.00
TOTAL			**S/ 408.50**

Tabla N° 2. Hardware y software

DESCRIPCION	CANTIDAD	TOTAL (S/)
Laptop HP 15 – Core I5, 8GB de RAM, Tarjeta Grafica Nvidia	01	S/ 0.00
Laptop DELL Inspiron, Core I3, 12 GB RAM, HDD 500 GB	01	S/ 0.00

Sistema operativo Windows 10	02	S/ 0.00
Visual Studio Comunity 2019 Versión 16.8.4	02	S/ 0.00
Corel Draw Grafics Suite 2020 Version Portable	01	S/ 0.00
SQL Server Management Studio 18.5	02	S/ 0.00
Suite Microsoft Office 2016	02	S/ 0.00
SPSS Statistics	02	S/ 0.00
Lector Bometrico ZK4500	01	S/ 329.00
Usb 8 Gb	02	S/ 32.00
TOTAL		**S/ 361.00**

Tabla N° 3. Servicios

DESCRIPCION	CANTIDAD	UNIDAD (S/)	TOTAL (S/)
Internet	12 meses	120.00	S/ 1440.00
Electricidad	12 meses	25.00	S/ 300.00
TOTAL			**S/ 1740.00**

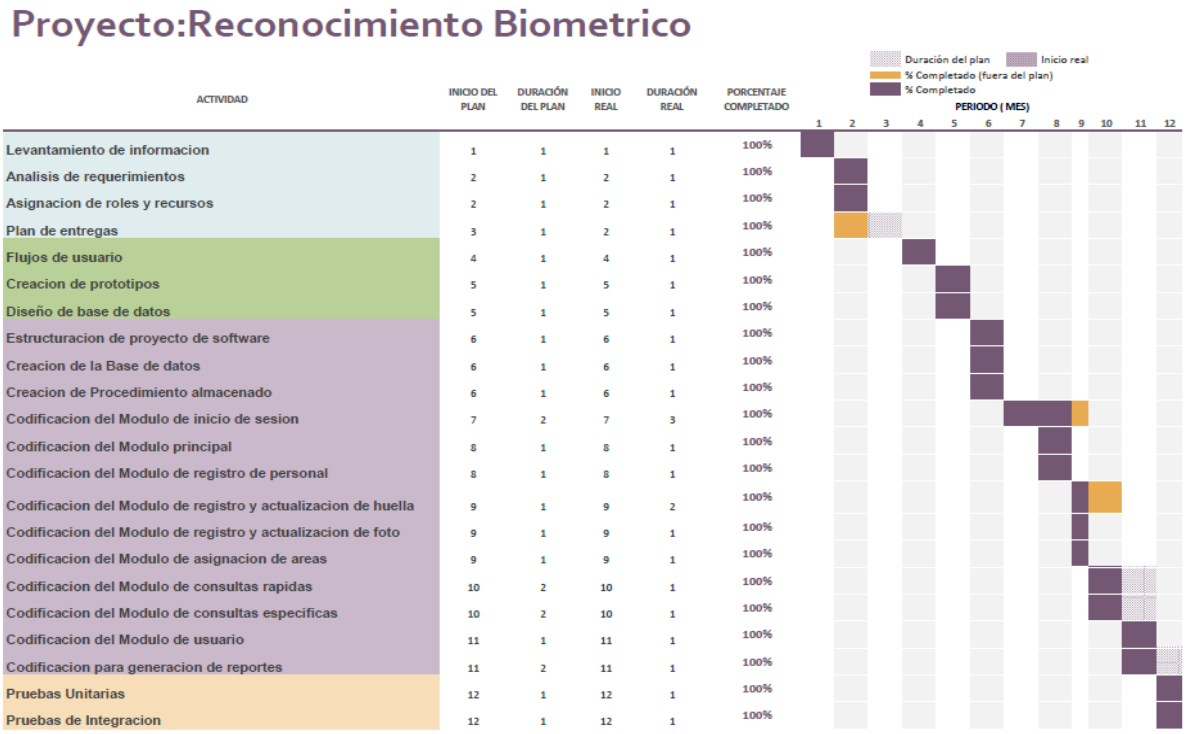


Figura 37. Cronograma de actividades.

Conclusiones

La metodología XP permitió cubrir los aspectos necesarios del proyecto, conforme a las especificaciones disponibles en relación a la información, recursos, tiempo, presupuesto e iteración con el usuario. Las fases proporcionadas para el desarrollo de software, se elaboró en base a una estructura organizativa dependiente del conocimiento que se obtuvo de los requerimientos y tiempos esperados por el usuario.

La aplicación del proceso de desarrollo ágil obtuvo un eficiente resultado en correlación con los objetivos planteados inicialmente, asimismo, estos resultados se sometieron a pruebas.

En el presente proyecto se conformó una unidad de levantamiento de información a través de precedentes y acciones relacionadas la observación directa, lo cual sirvió para poder estructurar las necesidades funcionales y no funcionales de todos los requerimientos encontrados. Posteriormente se elaboraron diseños en base a las características planteadas en la fase anterior a través de prototipos y estructuras de desarrollo. Por otro lado, el diseño fue realizado bajo el motor de base de datos SQL Server y la herramienta utilizada para su gestión fue SQL Server Management Studio 2016, proporcionando un entorno de trabajo ágil y ordenado.

Durante la fase de desarrollo se utilizó los programas Visual Studio en su versión 2020 bajo el marco de trabajo del lenguaje de programación C#, a través del cual se utilizó el paradigma de programación orientada a objetos POO.

Con respecto a la fase de pruebas se realizaron de acuerdo a cada módulo especifico de código obteniendo resultados favorables conforme a lo establecido en la fase de planificación.

Finalmente, aplicar la metodología XP en la creación de software, permitió la organización y entregas funcionalidades, de forma incremental. De manera se aprovechó el tiempo y recursos conllevando a una liberación de carga de trabajo innecesaria.

Referencias

Kendall, K., & Kendall, J. (2005). *Análisis y diseño de sistemas* (6ta ed.) México D.F, Mexico: Pearson Educación

Larman, C. (2002). *UML y Patrones.* Madrid, España: Pearson Educacion, S.A

Pressman, R. (2010). *Ingeniería del Software un Enfoque Práctico*. México D.F, México: McGraw-Hill

Sommerville, I. (2005). *Ingenieras de Software* (7ma ed.). Madrid, España: Pearson Educación.

Team, P. W. (2011). *Pear*. Recuperado el 3 de Septiembre de 2011, de PHPUnit: http://pear.php. net/package/PHPUnit/redirected

Wells, D. (1999).*User stories*. Recuperado el 3 de Septiembre de 2011, de user stories: http://www. extremeprogramming.org/rules/userstories.html