Universidad Norbert Wiener

FACULTAD DE INGENIERÍA Y NEGOCIOS
ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍAS

Tesis

Diseño de un modelo de control de accesos a los sistemas de información basado en la ISO 27001 en una financiera, Lima 2019.

Para optar el título profesional de Ingeniero de Sistemas e Informática

AUTORA

Br. Avalos Cárdenas, Carmen Victoria

LÍNEA DE INVESTIGACIÓN DE LA UNIVERSIDAD

Ingenierías de Sistemas e Informática, Industrial y Gestión Empresarial y Ambiental

LIMA - PERÚ

2019

“Diseño de un modelo de control de accesos a los sistemas de información basado en la ISO 27001 en una financiera, Lima 2019.”

Miembros del Jurado

Presidente del Jurado

Mg. Luis Enrique Ramirez Pacheco

Secretario

Dr. Davis Rivera Gómez

Vocal

Mtro. Nicolas Fedeberto Ortiz Vargas

Asesor Metodólogo

Mtro. Fernando Alexis Nolazco Labajos

Asesor Temático

Mg. Walter Amador Chávez Alvarado

Índice

Pág.

Pág.

Dedicatoria

A mis padres Carmen y Franklin agradezco su apoyo incondicional que siempre me han dado y que me han otorgado durante mi vida universitaria, para convertirme en una gran ingeniera.

Por último, a mi abuelito Pablo Avalos Navarro, que siempre con sus palabras y su confianza, me ayudo a lograr mis objetivos y ser siempre el orgullo de la familia Avalos.

Agradecimiento

A Dios por darme siempre fortaleza y bendiciones que me permitido enfrentar los obstáculos que he tenido.

A mis padres Carmen Cárdenas y Franklin Avalos, que con sus palabras y esfuerzo pude lograr mis objetivos.

Finalmente al Mg. Chávez Alvarado, Walter Amador, quien me asesoro y me guio durante la tesis, y también a los docentes de la Universidad Privada Norbert Wiener, que durante mi vida universitaria nos brindaron conocimientos y experiencias.

Declaración de autenticidad y responsabilidad

Yo, Avalos Cárdenas, Carmen Victoria identificado con DNI Nro. 75549670, domiciliado en Grano de Oro MZ H LT 16 egresado de la carrera profesional de Ingeniería de Sistemas e Informática he realizado la Tesis titulada "Diseño de un modelo de control de accesos a los sistemas de información basado en la ISO 27001 en una financiera, Lima 2019" para optar el título profesional de Ingeniero de Sistemas e Informática, para lo cual Declaro bajo juramento que:

1. El título de la Tesis ha sido creado por mi persona y no existe otro trabajo de investigación con igual denominación.

2. En la redacción del trabajo se ha considerado las citas y referencias con los respectivos autores.

3. Después de la revisión de la Tesis con el software Turnitin se declara 7% de coincidencias.

4. Para la recopilación de datos se ha solicitado la autorización respectiva a la empresa u organización, evidenciándose que la información presentada es real.

5. La propuesta presentada es original y propia del investigador no existiendo copia alguna.

6. En el caso de omisión, copia, plagio u otro hecho que perjudique a uno o varios autores es responsabilidad única de mi persona como investigador eximiendo de todo a la Universidad Privada Norbert Wiener y me someto a los procesos pertinentes originados por mi persona.

Firmado en Lima el día 24 de Julio del 2019

_____

Avalos Cárdenas, Carmen Victoria
DNI Nro. 75549670

Presentación

Señores miembros del Jurado:

El presente trabajo de investigación titulada “Diseño de un modelo de control de accesos a los sistemas de información basado en la ISO 27001 en una financiera, Lima 2019.”, tuvo como objetivo proponer controles y herramientas para que disminuya el incumplimiento de privacidad de información en la mejora del proceso de gestión de control de acceso en los sistemas y aplicaciones de la financiera, en la cual permite que la financiera pueda manejar herramientas y controles, para garantizar una buena gestión en el control de accesos de la financiera. El presente investigación se realizó para dar el cumplimiento al Reglamento de Grados y Títulos de la Universidad Privada Norbert Wiener con el propósito de optar el Título de Ingeniero de Sistemas e Informática.

La presente investigación está distribuida por seis capítulos, de la siguiente manera:

El primer capítulo se obtiene el problema de la investigación, donde se determina el problema general y específico, de las diferentes situaciones que hemos podido encontrar acerca de la seguridad de información referente a la gestión de control de accesos, obteniendo la justificación, los objetivos generales y específicos del problema.
En el segundo capítulo está referido al marco teórico, donde se encuentran las teorías donde fundamente al desarrollo de la investigación, podemos ver los antecedentes, que hemos encontrado a través de artículos, tesis, entre otros, y nos señala toda la información referente a la financiera.

En el tercer capítulo, nos señala la descripción de las categorías y subcategorías, se nos informa de la población, la muestra y las técnicas e instrumentos que vamos a usar para obtener los datos para llevar a un análisis.

En el cuarto capítulo, se describe el análisis que hemos obtenido de la entrevista y del cuestionario, resaltando la situación que tiene la financiera, llevando a una propuesta de solución. En el capítulo cinco, se describe la conclusión que hemos obtenido al usar la

alternativa solución que hemos sugerido, y detallamos sugerencias para que pueda de ser de gran ayuda a las financieras. En el capítulo seis, están las referencias bibliográficas, están los links de las páginas donde hemos obtenido información referente al problema que he desarrollado.

Carmen Victoria, Avalos Cárdenas
Dni: 75549670

Índice

Índice de Tablas

Pág.

Índice de figuras

Índice de cuadros

Pág.

Resumen

La presente investigación titulada “Diseño de un modelos de control de accesos a los sistemas de información basado en la ISO 27001 en una financiera, Lima 2019.”, se propuso como objetivo proponer controles y herramientas que disminuya el incumplimiento y vulnerabilidades de privacidad de información, para la mejora del proceso de gestión de control de acceso en los sistemas y aplicaciones de la financiera, con el propósito de evitar el robo y hurto de información confidencial, secreta e interna que tiene la financiera.

Por ende, en el desarrollo de este trabajo de investigación se realizó a través de instrumentos, en la cual se expresa las vulnerabilidades que pueden existir cuando el colaborador accede a los sistemas de información y comience a manejar o manipular activos que no le corresponde según su cargo.

Por el cual, con llevo a proponer herramientas automatizadas que controlen los perfiles que tienen los colaboradores cuando usen información confidencial, secreta e interna. También nuevos controles de accesos que apoye en la protección de los activos de información, siendo estas propuestas medidas que puedan originar confianza en el momento de manejar los datos de los clientes como: transacciones, historial bancario y datos personales de los clientes.

Palabras claves: seguridad de información, control de accesos, clientes, financiera, sistemas y aplicaciones, herramientas, controles.

Abstract

This research entitled “ Design of an access control models to the information systems based on the ISO 27001 in a financial one, Lima, 2019 “, it was proposed as objective to propose controls and tools to reduce the breach of privacy of Information in the improvement of the management process of access control in the systems and applications of the financial, in order to avoid the theft and theft of confidential, secret and internal information that has the financial.

Therefore, in the development of this research work was conducted through instruments, in which is expressed the vulnerabilities that may exist when the partner has access to the systems of information and begin handling or manipulate assets that it is not according to his position.

By which, i endeavor to propose automated tools that control profiles that have partners when using confidential information, secret and internal. Also new access controls that support in the protection of information assets, being these proposed measures that could lead to confidence in the time to handle the data of customers as: transactions, banking history and personal data of customers.

Keywords: information security, access control, clients, financial, systems and applications, tools, controls.

CAPITULO I
PROBLEMA DE LA INVESTIGACIÓN

1.1 Problema de investigación

Las empresas durante años han establecido normas y reglamentos en los diversos áreas de la organización para proteger los datos confidenciales de sus clientes y tener un control en los accesos que se le otorga a los colaboradores, en el momento de usar información confidencial, siendo un gran problema ya que se ha extraviado información interna que solo tienen accesos los colaboradores del banco, de manera que los clientes han perdido la seguridad y confianza al dar su información personal a una entidad financiera o/y empresa.

Cuando una persona abre una cuenta bancaria o registra sus datos personales en cualquier cuenta o servicio, esta entregado sus datos personales y confidenciales, otorgándole a la organización privilegios para poder transferir y manejar los datos de los clientes sin el consentimiento de los propietarios. El resguardo de los datos confidenciales de los clientes es un derecho fundamental que tiene la organización con él cliente. Este derecho quedo establecido en la Constitución Política del Perú en su artículo 2, numeral 6, donde la constitución identifica que toda persona debe tener los mismos servicios públicos o privados, considerando ciertas reglas como no compartir con personas terceras información privada y familiar del cliente. La manipulación y usurpación de la información, en el momento que acceden a sus datos, y la posibilidad de cambiarlos o borrarlos, ha llegado a superar el gran problema de robo de identidad, así que se estableció derechos para que fomenten respaldos en el mundo informático. Por un lado, las personas o clientes naturales deben prevenir que los datos personales que otorguen a un organismo privado o público deben estar adecuadamente gestionada por personas especializadas en la protección datos confidenciales de un usuario común.

Asimismo, el estado como parte de su labor debe efectuar la Ley N°29733 - Ley de Protección de Datos Personales – LPDP, el Estado requirió establecer lineamientos para la nueva regla a las personas naturales y jurídicas, que gestionen las de Base de Datos – BD de los clientes. Entre otras ejecuciones, para otorgar la Base de Datos al organismo nacional que protege los datos personales a dirección del Ministerio de Justicia y acorde a los responsables que están a cargo para el buen uso y manejo de la información no pública. Se determinó requerimientos para proteger el banco de datos que tienen las organizaciones,

para que en el momento de recopilar, registrar, almacenar, conservar, transferir, difundir y usar los datos personales del cliente, el propósito de los procedimientos es preservar las herramientas que llevan a cabo la protección de los datos de las personas naturales en las entidades bancarias y financieras. La finalidad que tiene la norma de cuidar los datos, es que el cliente maneje, disponga y decida sus datos personales con las precauciones que reglamente la ley N° 29733. La normativa impulsa multas a las empresas que incumplen faltas graves en la manipulación de los datos personales de los clientes, sin contar con la autorización de los principales titulares de la información que tiene el banco (Revista Ingeniería Nacional, 2017).

En España, se realizó un evento donde participo red seguridad, Instituto Nacional de Tecnologías de la Comunicación, RSA, entre otros, donde se comentó sobre la prevención en la perdida de información y el robo de información crítica, los expositores opinaron sobre experiencias ocurridas sobre la perdida, pero el tema principal fue fuga de información a partir de metadatos, se comentó esto, ya que existe personas malintencionadas que recurren a pagar con el objetivo de tener información confidencial. El tema se orientó sobre lo que se da en la actualidad, ya que muchos usuarios exponen su información importante en la red, y los daños serian irreparables, el expositor recomendó poner medidas para esquivar la fuga de información. También se comentó como medida de solución al problema la tecnología Data Loss Prevention (DLP), buena esta solución sería muy beneficioso en el cumplimiento normativo, pero según la revista esta medida no se puede adquirir ya que no existen una persona adecuada que se responsabilice en la manipulación de este sistema (Revista Red Seguridad, 2010).

Las entidades financieras siempre están en riesgos de la ciberataques, se informa que este sector siempre tiene mayor ataques en los equipo de TI, siendo una amenaza para la organización. Se informa que las financieras no pueden controlar las amenazas ya que no tienen herramientas automatizadas para disminuir este riesgo, llevando a una disminución en el ambiente laboral.

Los activos de información no han sido de gran importancia para este sector, pero con las nuevas regulaciones que existen, han tomado ser esto como de gran prioridad, ya que hay constante ataques, siendo esto de gran dificultad para la financiera, se informa que los ataques vienen cuando detectan sistemas vulnerables, practicas maliciosa, etc., cuando detectan un medio de acceso el atacante realiza el cambio en la información, siendo esto un gran amenaza para la organización, para garantizar una medida de solución, se debe reporta al comité de la organización, para que el comité reporte de la situación que tiene la organización, siendo la seguridad un tema que debe saber los colaboradores de la organización ya que ellos pueden correr el riesgo de ser atacado cuando manejan información (Revista byte, 2019).

La organización está extendidas sus redes para poder tener accesos a su información por medio de aplicaciones móviles y entorno a la nube, siendo estas herramientas dudosas, ya que se cree que estas herramientas están gestionadas y controladas constantemente por medio de la organización. Pero para controlar estas herramientas, se debe ver primero el control de acceso a la red, ya que se está cambiando las normas que existen en el mercado, pero para poder optimizar los riesgos hay que tener una mayor inversión en seguridad, como un sistemas de control de acceso a una nueva generación (NG - NAC) que permite visualizar a nuestra red interna, otorgando más seguridad en los dispositivos de la empresa, permitiendo establecer políticas y controles a los diversos eventos de riesgos, siendo este ventaja para toda la organización (Revista Red Seguridad, 2016).

Actualmente, en Lima las empresas bancarias y entidades financieras están de la mano con la Ley N° 29733 y mayormente el área de seguridad de información con la ISO 27001, ya que el área otorga conformidad a los colaboradores y a los nuevos ingresantes a tener acceso a diversas información secreta, confidencial e interna de los clientes, proveedores, entre otros, de manera que el área orienta a los colaboradores de todas las áreas de la entidad financiera que tengan cuidado en el momento que manipulen información, ya que siempre existen incumplimientos de loa colaboradores en el momento de ser uso de la información, siendo una amenazar para nuestra empresa, ya que nos

comprometemos a dar confianza y seguridad a sus clientes, cuando realicen el primer contacto con la empresa al disponer de su información personal.

1.2 Formulación del problema

1.2.1 Problema general

¿Cómo mejorar el control de accesos de los sistemas y aplicaciones en una entidad financiera, 2019?

1.2.2 Problemas específicos

¿Cómo es el control de accesos de los sistemas y aplicaciones en una entidad financiera, Lima 2019?

¿Cuáles son las causas de mayor amenaza en los controles de accesos de los sistemas y aplicaciones de una entidad financiera, 2019?

¿Cómo las estrategias influyen en el control de accesos de los sistemas y aplicaciones en una entidad financiera, 2019?

1.3 Justificación

1.3.1 Justificación metodológica

La búsqueda nos permitió conocer como es la gestión de control de accesos en las entidades financieras en Lima, realizando los métodos propuestos con el fin de realizar y elaborar una recomendación al inconveniente que existe en el departamento de riesgos sobre el incumplimiento de control de accesos que tiene los colaboradores en la financiera. Asimismo, podemos dar un beneficio a los clientes que confían cuando brindan su información personal a la financiera, otorgando al área herramientas y controles para detectar los incumplimientos que tienen los colaboradores en el momento que pueden acceder a sistema y aplicaciones de la empresa.

1.3.2 Justificación práctica

Los objetivos que se asignaron en nuestra investigación, nos permite tomar decisiones para disminuir las amenazas que existen en el área, debilitando los controles existentes que nos está perjudicando y dañando la información de la empresa, de manera que según el problema nos está permitiendo encontrar soluciones para la gestión de control de accesos de los sistemas y aplicaciones en una financiera, Lima. Los resultados observados durante nuestra investigación nos van otorgar información para poner en funcionamientos las herramientas y controles que requiere la gestión de control de accesos de los sistemas y aplicaciones en una financiera, Lima.

1.3.3 Justificación teórica

Para poder comenzar a plasmar nuestra investigación hemos encontrado teorías que nos van a dar información para poder defender la idea que nos va a llevar a una solución. Las teorías que han sido asignadas según nuestro problema de investigación, es la teoría desarrollo organizacional, lo podemos visualizar en el área de riesgos; también la teoría de información, la teoría de seguridad de información, la teoría general de sistemas y la teoría de mosaicos que especifica la transacción de datos e información privada de las personas naturales, desarrollando medidas para que el colaborador que labora en la entidad financiera tenga controles durante el uso de la información privada que nos otorga el cliente.

1.4 Limitaciones

El mayor aporte que hemos observado durante nuestro plan de investigación, es el tiempo que tomamos en nuestra investigación, cuando comenzamos a iniciar y plasmar la información. También, hemos encontrado obstáculos en el momento de buscar información de la ISO 27001:2014.

1.5 Objetivos

1.5.1 Objetivo general

Proponer controles y herramientas que disminuya el incumplimiento de privacidad de la información en la mejora del proceso de gestión de control de accesos a los sistemas y aplicaciones en las financieras de Lima, 2019.

1.5.2 Objetivos específicos

Diagnosticar la posición de la gestión de control de accesos de los sistemas y aplicación en la financiera de Lima, 2019.

Explicar las causas de mayor importancia que ocasionan vulnerabilidades en la gestión de control de accesos de los sistemas y aplicaciones en una entidad financiera, 2019

Predecir la influencia de las estrategias en la gestión de control de accesos de los sistemas y aplicaciones en una entidad financiera, 2019

CAPITULO II
MARCO TEÓRICO

2.1 Sustento teórico

Teoría General de Sistemas

Se determina que la teoría tiene una complejidad de componentes para caracterizar información, tácticas, métodos y procedimientos para puntualizar mejores decisiones en los novedosos recursos explicativo e informativos (Bertalanffy, 1976).

Por ello el sistema que se va implementar, va eliminar la vulnerabilidad, debilidades que puede afectar a la corporación y a nuestra división, con las nuevas decisiones se va poder solucionar los problemas o brechas que tiene la división para llegar a una solución.

Es decir, la implementación de una metodología de sistemas en la empresa, puede enriquecer las ganancias, producción, beneficiando a la empresa a cooperar con la asistencia de los requerimientos que demandan los usuarios (Tamayo, 1999).

En el momento de ser uso de la metodología de sistemas se puede reducir las amenazas críticas que repercute en las actividades de los colaboradores de la empresa, ampliando la imagen corporativa ante el público.

La teoría general de sistemas se define por un sistema abierto y cerrado, teniendo el sistema abierto medio para relacionarse entre otros sistemas, viendo diversas conexiones y transacciones de datos, y el sistema cerrado se define por no tener comunicación o conexión con otro equipo (Arabany, 2002).

Los sistemas que se expresa abierto y cerrado, se puede ver que los diversos sistemas pueden tener transacciones de datos e información teniendo accesos o no accesos a los usuarios.

Expresa que la teoría general de sistemas se ha hecho por medio de procesos, que durante los cambios o rediseño que sufre la organización puede sufrir cambios en la información, en los objetos, y tiempo en las actividades de la organización (Sarabia, 1995).

La teoría define que la dinámica que sufre de los sistemas puede sufrir cambios en los procesos por las funciones que realizan los usuarios o por las necesidades que requiere la persona en momento que usa un sistema.

La teoría se ha originado por las diversos cambios que ocurre en los sistemas, ya que los sistemas puede desarrollar diversas actividades, que cambie los labores de los usuarios, para que ellos pueden tomar una buena decisión en el momento que sucede un problema en la época moderna y tecnológicas (Torres, 1996).

Para llevar a cabo cambios en los sistemas, se requiere ver la necesidad para que el líder puede las funciones que requiere, siendo esto necesario, para que pueda asumir responsabilidades y decisiones antes los problemas que se ve en la vida real y profesional.

Teoría del Mosaico

La teoría pronuncia que la información privada y pública, es función que conserva la persona y la utilidad que le da el otro usuario que gestiona la información. De manera que la información es sumamente importante siendo está protegida por el hurto y robo de información (Ruiz, 1994).

La teoría nos permite reconocer que la información secreta y confidencial, que manipule el colaborador debe contar con normas de LPD para evitar la mala manipulación de la información que se está manejando en el ente financiero.

Se determinó que, en los medios de comunicación, pueden existir personas que vulneren y expongan la información personal de otros usuarios, siendo alterada y modificada para beneficios monetarios (Calderón, 2009).

La teoría permite diferenciar las amenazas que se arriesga la persona al subir por medios de comunicación sus datos personales y secretos, siendo una terrible exposición de los usuarios, llevando a que las personas roben la identidad de otros.

La teoría del mosaico consiste que un usuario cuando envía o guarda información a la red, muestra al mundo y a diferentes personas tu personalidad, poniendo en riesgo tu información personal (Herrera, 2016). Nuestra investigación consiste en sobre guardar la información de los clientes a través de modelos y estrategias para que nuestros colaboradores tenga un mejor uso de la información.

Podemos ver que la teoría del mosaico se muestra a través de información que debe guardar datos de la persona, teniendo que cerrar la conectividad de los datos con el ciberespacio para evitar la trazabilidad de la información (Alcala, 1998).

La investigación define que las entidades financieras mantienen un espacio protegido para nuestra información, siendo posible la legitimidad de los datos que se maneja en los centros financieros.

Se verifica que la teoría del mosaico se puede ver a través de experiencias y conocimiento, que se vuelva un proceso que proceda a jerarquizar actividades o funciones, reflejando modelos para que ocurra conexiones entre modelos (Miranda, 2012).

El proceso cuando se organiza y se jerarquiza lleva a una investigación a poder definir diferentes estrategias para estructurar un sistema que pueda llevar una solución la investigación.

Teoría de la Información

Por lo que se refiere la teoría que las diversas dificultades tienen en los sistemas representa el estado por la coordinación que tienen los conectores para obtener una información resguardada durante el proceso (Johansen, 1982).

La teoría permite ver que los sistemas tienen en el interno diversos complejos de rangos, que mediante la operación, la información que tiene debe ser conservada durante los procesos de protección de datos que tienen la empresa.

En la teoría se explica que un número corto en la codificación no puede representar una pérdida de información, pero si el mensaje es grande en la fuente de datos seria expuesto a la perdida de información (Lopez y Veiga, 2002).

Explica que los mensajes cortos o largos en la fuente de datos de cualquier entidad puede originar una pérdida de información, siendo una gran amenaza para la entidad, de manera que el dato es fundamental para dar el seguimiento a un cliente.

La teoría de la información define que es una conexión entre la información o datos semejantes, viendo que las descripciones de la información sean semejantes, siendo esta no información alteradas que reflejen errores, teniendo medio para verificar que todo lo expuesto en la información es auténtico y claro (Uscatescu, 1973).

La investigación que hemos realizado para poder llegar a una solución se debe tener información, claros y precisos para poder llegar a una solución que resuelva el problema que tienen las entidades financieras.

Con la teoría de la información podemos encontrar códigos que pueden transmitir medios para poder tener conexión, dando al usuario medios para que acoja el mensaje enviado, siendo estas conexiones maneras de recibir comunicación e información de los procesos, siendo este medio confiable y discreto ante las conexiones (Cuenca, 1999).

La investigación lo que trata es que los colaboradores de diversas áreas tengas maneras de tener accesos a los diferentes sistemas, en sentido optimo y confiable, ya que la información que nos otorgar ha sido guardado transparentemente.

La teoría trata de explicar que la información puede ser expresada a través de datos, iconos, números, para cubrir el principal mensaje que tiene la información, siendo la expresión segura en la longitud de los datos que representa para ver el mensaje (Garcia & Fernandez, 2002).

La información que manipule un usuario debe tener medios para poder proteger la información confidencial y secreta de la organización, siendo esto nuestra mayor vista para cuidar nuestro mensaje que otorga la información.

Teoría de Desarrollo Organizacional

En cuanto al desarrollo organizacional se manifiesta en la reparación del problema, orientando a los usuarios a identificar medidas estratégicas ante una dificultad, retroalimentando a los usuarios a capturar mejores decisiones (Montufar, 2013).

Define que para reparar un incidente hay que observar y dar una solución al problema que pone en riesgo a la empresa, de manera que con la ayuda de la toma de decisiones se pueda adaptar a los diversos ataques tecnológicos y estructurales.

En la teoría el desarrollo organizacional define que la mejora de un proceso que representa a la empresa para el crecimiento de sus actividades y el éxito de sus objetivos (Gallarzo, Espinoza & Hernandez, 2011).

En definitiva, la mejora del proceso de la empresa representa el equilibrio de sus actividades para incrementar la protección que beneficiara un gran resultado en sus objetivos que acorda cada área de la entidad.

La teoría desarrollo organizacional es conformado a través de formas que define relación con diferentes campos o áreas del sistema, siendo este medio una conexión con las diversos objetivos que tiene los eventos o hechos que sucede en la organización (Gallarzo, Espinoza & Hernandez, 2011).

En la investigación nos muestra que debemos tener relación con las áreas y los procesos que tiene la financiera, ya que con la ayuda de ellos definiremos los accesos que deben tener sus colegas.

Se identifica que la teoría de desarrollo organizacional se realiza modificaciones ya que nos ayuda a crear; modernidad, transformación y una variación minuciosa, siendo excelentes para la norma administrativa, significando el reconocimiento de los eventos de gran riesgos o perdida que tiene la compañía (Moguel, 2012).

Siempre una nuevo desarrollo y metodología es una señal de cambio que lleva a levantar principales eventos que arriesgan nuestro sistema, o medio donde accedimos nuestra información, siendo esto un hecho primordial de la investigación.

La teoría de desarrollo organizacional señala que formarse de los problemas que ocurren en el nuestro centro laboral, es una forma de adquirir conocimiento, siendo este mecanismo la manera de alimentar nuestros fundamentos, que nos lleva a observar un novedoso entendimiento del desarrollo organizacional (Dailey. 1990).

La investigación nos lleva a captar nuevos medios para poder solucionar riesgos, amenazas, eventos de perdida en el capital de la entidad y problemas que tienen el área de seguridad de información de una financiera.

Teoría de Control

Siendo la teoría de control un método de poder inspeccionar un procedimiento del sistema, para siga manejando con indicadores específicos, siendo este examen un grupo de herramientas que trabaja de manera vertical para tener un resultado o una contestación (Carrillo, 2011). En la investigación nos muestra que los sistemas es el recurso primordial, que lleva a los sistemas ser un factor para llevar a la manipulación de la información.

La teoría de control nos permite identificar estrategias de reparo, para poder crear a los sistemas una función uniforme, que pueda enmendar el grupo de solicitudes activos o las peticiones injustificadas (Perez, Hidaldo y Berenguer, 2008).

El control nos permite poner en práctica a los sistemas las diferentes solicitudes importantes que requieren las áreas, siendo este medio un método de observar las peticiones que más necesitan.

Una función conlleva a que la teoría de control tenga una etapa usual, en sus actividades siendo esto modificada por el transcurso del tiempo, que conlleva a crear estado o ciclos que pueda estar considerados en los sistemas (Tocancipa, 1976).

El proceso nos lleva con el tiempo a poder ver rediseños o cambios en los sistemas, considerando esto un medio para eliminar o atacar las nuevas amenazas, siendo que estas puedan obtener información confidencial o secreta de las entidades financieras.

Analizar la teoría de control conlleva a verificar las variedades de sistemas, siendo esto una forma de conocer que el sistema desde su etapa original, a su ciclo definitivo, se ha definido pautas o trabas para llevar a un buen estado de control de este (Cerpa, 2009).

En el estudio nos presenta que para poder acceder a los sistemas debemos tener definidos los perfiles para poder manejar la información, teniendo que ver que los sistemas tengan claros los perfiles que tienen los colaboradores.

En la teoría de control maneja variante que conlleva a analizar el concepto que tienen las distinciones, teniendo el beneficio de que el costo pueda tener un cambio extraordinario, pero vemos que el costo puede representar una distinción deseada (Smith y Corripio, 1991).

En nuestro estudio tener control de los sistemas que maneja los colaboradores conlleva que los perfiles que tienen los usuarios es el valor que permite acceder a diversos documentos que fomentan la comunicación de la información obtenida.

2.2 Antecedentes

Internacional

Según Valencia y Orozco (2017), en el artículo nominado *Metodología para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 2700*, cuyo objetivo es plantear un sistemas de gestión de seguridad de información explicando los principales bases de las normas iso, dando la comparación entre seguridad de información y seguridad informática, aportando a la organización un motivo decisivo en la SGSI. Al final del artículo, se concluyó que las alternativas para establecer un buen accionamiento en la gestión de seguridad de información que se entabla por procesos complejos para el establecimiento de un proceso metodológico, otorgándole una interrelación que existe con las diversas normas de la iso, para encaminar con los estándares que existen a la organización, siendo este medio para abordar proyectos que precisen los profesionales.

Según Acosta (2015), la investigación *Desarrollo de un modelo de seguridad para la prevención de pérdida de datos dlp, en empresas pymes*, siendo el objetivo definir un boceto de seguridad de información para llevar a cabo la custodia de los datos en las pequeñas y medianas empresa, siendo una herramienta que prevé el extravió de la información sociedades pymes. En la investigación se describe la metodología descriptiva debido a que incluye un estudio inductiva, deductiva y experimental, se llevó a cabo el sistema DLP endpoint en la organización. Con la ayuda de la metodología deductiva se podrá validar y reconocer los eventos problemáticos que está ejecutando en la empresa actualmente. La investigación les permitió concluir, que el extravió de información de la organización puede generar un daño en la información que tiene la empresa, se explicó dos obstáculos: el fallo tecnológico y la dificulta humana. Se infiere que la ejecución del boceto para la custodia de los datos ha sido satisfactorio, ya que se podido disminuir los conceptos tecnológicos que opera en tiempo real la información de la empresa.

Según Sanz (2015), en el artículo nombrado *Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado.* El articulo definió como objetivo, que el estado deben publiquen de manera indefinida información sin controlar las peticiones de los usuarios, como la opción de mostrar, esta realidad se centra en la claridad activa, y por último se tomó como objetivo que los organismos públicos, en unión con la información está en su poder que el reglamento no obliga al publicar, otorgar datos que sean de gran importancia por el ciudadano (teniendo en claro que no debe ser usada la información privada del usuario), la realidad es que el derecho a obtener acceso a dicha información pública, que según se define en otorgarles derechos o permitir y saber. En consecuencia, cuando se obtiene acceso a la información de otro usuario se verifica técnicas para lograr una mejor transparencia en usuario común. Al final, se determinó que el acceso a la información privada de un usuario común es un derecho que debe tener el individuo y cualquier otra persona, para investigar u obtener los datos que necesitamos (con independencia constancia y control de los expedientes) en poder de cualquier ente o persona pública, de cualquier sociedad, grupo o corporación privado o independiente de la propiedad del estado o siendo controlado por él, y de alguna cooperativa particular (con el trato de que la empresa reciba apoyo común o que tengan labores y funciones cotidianas, pero solo con respecto a las bases o asistencia públicos realizado, para el buen funcionamiento de nuestro país y de los datos que dan un persona común ante la sociedad), la conexión deber ser bloqueado por privilegios taxativas que respecten el reglamentos de una colectividad demócrata.

Según Aparicio (2017), el articulo denominado *Conceptos y legislación de transparencia sindical y protección de datos personales de los trabajadores en México*, el objetivo del artículo es obtener un eficaz y eficiente ejercicio para las actividades de las organizaciones, y evaluar que estos objetivos se cumpla según su creación, es decir: la investigación, mejoramiento y la protección del grupo del sindicato. El trabajo de estudio se concluyó que la espera que tiene la transparencia sindical sirva como un medio de instrumento que ejercer los derechos de los obreros, como los principales actores que ejercen una función importante en el área laboral siendo su deber obtener un negociación social, para llevar a cabo se debe respetar sus derechos laborales; y no sea una herramienta

para dificultar la claridad, siendo un modo de sanción a las agremiados exteriores que tienen intereses organizacionales, eliminando los pocos grupo sindicales independiente. Sin embargo, el tema de reguardo de los datos de los trabajadores es el principal situación, así como el trato que otorga la empresa a los trabajadores. Por consiguiente, las nombradas "listas negras" se muestran como una alerta del mal funcionamiento que se tiene en el uso de los datos de los trabajadores, para restringir la comunicación de los empleados a sus compañeros de trabajo. De manera que, los propios sindicatos tienen la obligación de mantener una clara información sindical, sino también en el cuidado de sus datos que tienen en a su custodia, y como se ha visto en la investigación, muy poco se ha comentado sobre este tema.

Según Monsalve (2016), el artículo nominado *La Protección de Datos de Carácter Personal en los Contratos Electrónicos con Consumidores: Análisis de la Legislación Colombiana y de los Principales Referentes Europeos*, el objetivo que definió el artículo es examinar el contexto que regula el estado colombiano que se aplica a los eventos de los datos confidenciales de los consumidores que son ingresado por un usuario al sistema que se manifiesta en un contrato electrónico, siendo como conocimiento a los directivos que están al máximo rango de la legislación europea. Al final del estudio el reglamento de los datos personales que tiene como propósito resguardar la información de los consumidores y la sociedad viene a fortalecer los registros digitales y/o electrónicos el compromiso de otorgar a la información precontractual y pos-contractual que ha sido debilitado por los agentes o vendedor, por ser impuestos a manifestar la determinación del proceso de expedientes particulares obtenidos por el manejo de los contrato, con miras a establecer una aprobación y permiso independiente, definido o comunicado por los clientes y proporcionar autenticidad y claridad en el momento del recaudo e gestión de la investigación de los datos privados de los clientes.

Según Tola (2015), la investigación bajo el titulo *Implementación de un sistema de Gestión de la Seguridad de la Información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001*, tiene el objetivo de promulgar un sistema de gestión de seguridad de la información para defender la reserva, integridad y existencias de los

testimonios de la empresa A&CGroup S.A., la metodología que se refleja en la investigación en sobre el PDCA (Plan-Do-Check-Act) y la metodología MAGERIT en la que considera un tácticas sistemáticos que permita examinar los eventos, iniciando medios para un buen resultado. La investigación llevo a la conclusión, que cuando hallamos sucesos inseguros coloca a los activos de información a una exhibición causando pérdidas siendo imprescindible asignar controles, con el fin de custodiar los activos de información. También, es significativo fijar régimen y directrices que encaminen a la organización a propiciar su información.

Nacional

Según Alvarado (2016), el articulo denominado *La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales*, siendo el propósito de favorecer un inserción de un proceso de evaluación continua, por medio de la clasificación de los conjunto de datos de los clientes que tienen la empresa en comprensión a los riesgos que se está midiendo la susceptibilidad y método dado a esta investigación, que se añade a los procesos técnicos, orientar a los usuarios naturales que usen en su ambiente laboral y profesional una protección, y solicitar un grado de seguridad que provee los riesgos, los métodos de seguridad y el precio de los métodos que se está incorporando a esta medida. En este artículo está orientada a una metodología que sigue diversos principios propios a equipos de gran alta de profesionalismo que hoy en día son archivados en forma de códigos, políticas o actas de eventos que hacen más común la asociación entre el ambiente profesional y legal. Como resultado obtenidos en la investigación, se obtuvo que seguir ciertos dominios de defensa ante los peligros de ataque que no se obtiene hoy en día como resultado de un método que va observando las debilidades y peligros latentes que van causando ciertos eventos de deterioro o destrucción en el ambiente. En definitiva se concluyó, que la gestión de evaluación continua va distinguir las debilidades y señal de peligros, motivos y la posibilidad de que vuelva a suceder y el agravia que provocaría .En definitiva incorporar ciertos dimensiones de seguridad es determinada por el incremento de registros y ubicuidad del conjunto de datos que tiene la empresa, el valor y el manejo de los datos por cada individuo, el periodo de su procedimiento y el compromiso del titular del conjunto de datos.

Según Eguiguren (2015), en el artículo bajo el titulo *El derecho a la protección de Datos Personales Algunos temas relevantes de su regulación en el Perú*, cuyo objetivo de la ley de los derechos de los datos personales es aplicar que toda información, inscripción, formato, expedientes, conjunto de datos personales que sea ha establecido como una tarea financiera, científica, de estudio entre otros; definida al puesto de la sociedad pública o privada., puede ser protegida si tiene como titula a una persona natural para el manejo de la sociedad privada o pública, siendo este medio para la asignación de las capacidades organizacionales, en función a defensa nacional, protección pública y medida penal para el estudio y sometimiento del delito. Al final es estudio permitió que se reconozca y se sugiera constitucionalmente una optimización a los derechos confidenciales que tiene cada persona en su vida privada, siendo este flujo como un medio de crecimiento a las nuevas innovaciones que tiene la era tecnológica de la información. El cuidado y medición es evento primordial para otorgar al titular o al cliente el derecho de tener el máximo fase de control y decisión autónoma sobre la información privada y datos a su persona.

Según Haza (2015), en el artículo denominada *No se lo Digas a nadie, pero tengo un banco de Datos de Clientes Sensibles, La Gestión de la Protección de Datos de Personales en el Sistemas Financiero para la Prevención de Lavado de Activos.*, en el objetivo del artículo es mostrar que no está dispuesto ejecutar la Ley de Protección de Datos Personales que toma referencia a los usuarios débiles y al público que denominado PEP, llamados usuarios que son expuesto públicamente en el contenido de la precaución de blanqueo de dinero. De manera, en el artículo se manipulo la metodología de innovadores paradigmas que lo podemos encontrar a través de la creación de metodologías que hallen y evalúen los riesgos, así también el resguardo de los documentos confidenciales de los usuarios que está definido en las normas de los clientes que tiene definido la organización. La sugerencia que se define en el artículo es exponer un ensayo que explique las recientes paradigmas que puntualice el reguardo de los datos de los clientes, claridad y valides en el proceso de la información y la unión que tiene los expedientes de los clientes con la gestión de riesgos. Se pudo concluir en el artículo que al otorgar custodia a los expedientes de los clientes es fundamental el secreto de la información de una cliente natural, que puede ser a partir de un paradigma erróneo, la responsabilidad de encargase de que todos los clientes

sean beneficiados de tener un buen resguardo que requiera la protección de un órgano nacional que se responsabilice de mantener el cuidado de su privacidad de las personas más allá de la autoridad que tenga en el estado, dedicar una buen custodio para la información se puede entender que la información pública para el estado no siempre va ser para el manejo y uso de su poder.

Según Aguirre (2014), el trabajo denominado *Diseño de un Sistema de Gestión de Seguridad de Información para servicios Postales del Perú S.A.,* la investigación tuvo por objetivo proyectar un sistema de administración de defensa al aclarar para SERPOST según lo indicado por la ISO/IEC 27001:2008 y la NTP-ISO/IEC 17999:2007 de seguridad de información. En la metodología que resalta la investigación es brindar la asistencia de las peticiones para establecer una organización de administración de defensa a la información, se utilizó el ciclo de DEMING, o también llamado circulo PDCA, Plan – Do – Check - Act, durante el estudio se manejó una metodología cíclica, que es siempre utilizada por la Organización Internacional de Normalización relacionada siempre con los reglamentos de las diferentes gestiones que la organización administra. Sin embargo, se visualizó una gran ayuda del comité debido que si el mando del grupo no se podría llevar a cabo el funcionamiento de las decisiones del equipo de trabajo, bajo los métodos, procesos y procedimientos de las normas de defensa de la empresa, ya que explica que controles se puede ejecutar durante un riesgo o amenaza, los talleres o difusiones son un medio de culturización a los colaboradores, siendo su función de manejar las normas dentro de sus área laboral, para llevar a cabo la incorporación de SGSI en nuestra empresa, se tiene que realizar los debidos normas internacionales a defensa a la información de los colaboradores, el punto que se pronuncia es una herramienta de buena práctica, ya que podemos asegurarnos que el uso y el manejo va ser eficiente en las distintas de áreas de la empresa. Al finalizar el estudio concluyo, que para implementar es de buen uso orientar los métodos y procedimientos de seguridad y defensa que están ahora en el mundo empresarial, debido al poco conocimiento que tiene los colaboradores para ejecutarlo en su empresa.

Según Espinoza (2013), en estudio nominado *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo,* en el estudio se definió como objetivo examinar y trazar una técnica de proceso de seguridad de información, apoyado por organización de estandarización ISO/IEC 27001:2005, para llevar a cabo a una organización dedicado a la fabricación y negociación. La metodología que se usó en la investigación es nombrada MAGERIT II es un método para organizar y encontrar amenazas que pueden ser las principales amenazas que vulneren y debiliten a nuestra organización, el gran aporte que nos va dar este método es que nuestra área podrá examinar las vulnerabilidades y podrá levantar las medidas, para mantener bajo fiscalización nuestros estado de riesgo. Nuestro estudio ha concluido que la técnica de proceso de seguridad a favor de la defensa de la información se organiza a los controles que tiene la gestión de fabricación y negociación que tiene actualmente la empresa, se debe coordinar con el responsables o usuarios de los procesos que fueron evaluado para la técnica de defensa al cuidado de la información de este investigación, la seguridad tiene que ser un tema de mayor interés para darle mayor importancia a la seguridad de la información, y para levantar las amenazas que pueden ser un peligro a la información que usamos diariamente en la empresa, de esta manera se debería coordinar de tomar planes de acciones sobre posibles amenazas.

Según Rivas (2016), su estudio nominado *Implementación de un sistema de control de acceso para mejorar la seguridad de información de la empresa SNX S.A.C*., el objetivo del estudio es imponer un sistema de control de acceso para perfeccionar la seguridad de información de la organización, afianzando una estabilidad en su información a los involucrados de la organización. El estudio concluyo que la conformación de una muestra de los accesos cuando se incorpora por roles es laborioso, pero puede ser explicados por los atenciones que solicitan los usuarios.

2.3 Marco conceptual

Categoría: Gestión de Control de Accesos

La teoría de gestión de control de accesos explica que los accesos son monitoreados a través exenciones especiales para conectarse con la información que va usar, llevando un grado de inspección en las opciones del perfil según al cargo que tiene el colaborador. De manera que, si conocen el manual de procedimiento y procesos de las áreas responsables, podrán usar responsablemente la información en la organización (Carazo, 2013).

La investigación se basa en la verificación y monitoreo de los accesos que se le otorga a un colaborador, con ciertas restricciones, encargando a un responsable que tenga un control en los sistemas de la financiera.

El sistema electrónico se define como una gestión de control de accesos, ya que bloquea y concede vías de conexión al usuario a las fuentes de información, dando ciertas validaciones para verificar que es el usuario indicado, la validación se realiza por diversas fuentes de lectura (lector de tarjetas, huella digital, etc.) y tiene un monitoreo que inspecciona las herramientas por medio de un programa. Para otorgar autorizaciones correctos es necesario de requerimientos específicos (Mora, 2016).

Por medio del control de accesos se otorga a los colaboradores ciertas medidas de restricciones y les concedes accesos a las informaciones que van a manejar para determinadas funciones que cumple según su cargo, dando herramientas para que pueda acceder con seguridad con las diversos maquinas, programas y aplicaciones de seguridad.

La gestión de control de accesos en palabra deduce como se compone los procedimientos de intereses científicos, arquitectónicos y gubernamentales que efectúa la misión de diligencia de la analogía del usufructuario y contrastar el acercamiento de los distintos tácticas de la entidades (Montoya y Restrejo, 2012). El flujo que abarca el desarrollo del control de acceso es el panorama de los modelos que representa la conexión de los beneficiarios hacia los distintos portales que puedan alcanzar.

Coincidir con el estudio a modo de dirigir la inspección a través de acoger una forma para probar que la constitución caracteriza encarar con notoriedad la contingencia del comercio (Dextre y Del Pozo, 2012).

El estudio que efectuamos contrarresta observa de modo muy minucioso, alcanzar un ejemplo, que nos avale el dominio que tiene los eventos de perdida en el negocio.

Establecer un sensato disposición de los sectores a través de sus cumplimientos, orientando este medio para cada campo consintiéndole información de sus éxitos y aportación concerniente al cometido de su acción en la firma (Cedeño y Muñoz, 2000).

El crecimiento que tienen las áreas de cada departamento es el medio para poder involucrar esquemas o propuestas a los colaboradores de enriquecer sus funciones.

Subcategorías:

Subcategoría 1. Políticas de Accesos

Las políticas de accesos son flexibles a la corporación, de manera que los resultados que tienen los responsables de otorgar accesos, se tienen incorporado las políticas de instrumentos para poder brindar accesos a los nuevos usuarios que tengan contacto con documentos virtuales, necesitando conformidad de los requerimientos atendidos (IBM, 2012).

En la investigación las políticas es un control que tienen que cumplir lo colaboradores en el momento de encontrarse en eventos que arriesguen la perdida de información o vulneración de datos.

La políticas de acceso consiente a definir internautas a ejercer conglomerados de encuentros unidos a ingenios, formalizando valerosos requisitos (Carrión, Fernández y Toval, 2011). En el despliegue de la exploración las reglas o normas que se emprenden en sistemas o entidades son importantes puntos que visualizan los dictámenes del colaborador.

La política promulga acciones ejecutadas, a través de actividades políticas, para absolver hechos que solo son importantes en dichos sectores y no son ejecutadas en el ámbito privado. Surge como evento de un proceso, siendo compuesto por decisiones, de una entidad pública, por periodo y en un lugar, frente a las situaciones que vive la población (Cardozo, 2013).

Acerca de la promulgación de una política, que es definida por el comité del área o el departamento, es importante activar dicha política para absolver riesgos que se está observando en una entidad bancaria o financiera, orientando a los colaboradores de que al activar es ejecutar en el ambiente laboral.

Las políticas definen el modelo para organizar las cosas y arregla los procesos. Recordar de las prohibiciones y del obstáculo de la tecnología es comprender lo primordial de las políticas. La política traza un camino para operar un evento problemático. Teniendo las políticas damos a los colaboradores medios para que tomen las decisiones que surgen en las actividades del día y mañana (Dussan, 2006).

Por lo que se refiere a las políticas que se crean en la empresa son procedimiento que tiene que seguir el colaborador ante una situación problemática, siendo estas políticas, una información importante que se tomara en una situación cotidiana y futura que tiene el empleado con la empresa.

Las políticas de acceso se alcanza interviniendo instauraciones de un conjunto de inspecciones que engloba tácticas, métodos, configuraciones administrativas y cumulo de componentes físico e ordenes que guie al procesador (Baluja y Porven, 2013).

Para la aplicación de un modelo, se requiere que intervengan auditores que reconozcan que régimen o regla exige el bosquejo, para conducir a los vínculos que poseerían los funcionarios.

Indicadores

Disponibilidad

La disponibilidad especifica el derecho de periodo en que labor esté preparado para asumir sus funciones o elaborar en estructuras que efectúen diariamente (Mesa, Ortiz y Pinzón, 2006).

En la ejecución de nuestra propuesta se requiere el derecho de adquirir y tener el recurso de tener continuamente los reportes o informes que requerimos.

Seguridad

La seguridad se puede representar como una norma llamada Tecnología de la comunicación y/o información, siendo una técnica de seguridad para operar, resguarda, evaluar, arreglar y conservar el sistema de seguridad de la información, completamente legalizado. La ejecución de las peticiones de esta regla deja que la compañía tenga el poder de tener la certificación internacional (Valencia-Duque & Orozco-Alzate, 2017).

Esta definición concuerda con la tesis, ya que la gestión de seguridad de información define que para mantener segura nuestra información hay que ejecutar medios para validar, monitorear, revisar y tener una mejora operacional, en el momento de confirmar que la información que tenemos es sumamente confiable.

Accesos de Seguridad

Las amenazas que se detecta generando debilidad en la empresa, debe iniciar con un plan de acción, dando frente a la debilidad. El plan de acción que se usa en el Sistema de seguridad de información debe abarcar los alineamientos que tiene la empresa, los accesos, los responsables y las normas que sigue la empresa para garantizar que el SGSI sea ejecutado constantemente (Ruben, Yupanqui & Bayone, 2015).

Las amenazas son hechos que repercute económicamente y funcionalmente en la empresa, pero en la ejecución de la SGSI, se inicia con el plan de acción, para tener medidas de control cuando ocurra un incidente o evento de amenaza.

Subcategoría 2. Control de Accesos

El control de acceso manifiesta que la región del comercio ha hallado un cumulo de estatus que normaliza la marcha de la actividad con la firmeza, para vigilar la dirección (Revista Gerencia, 2010). En el estudio propuesto el control de acceso se explaya al delegar estatus a los modelos, actividades a desarrollar.

Notificar tolerantemente restricciones en la variación que reportar autorización, exige minuciosamente fijar anuencia apropiada de cada individuo (Mora, 2016). Para requerir una variación de un perfil en los modelos o diseños se exige un consenso de los departamentos, para efectuar la eventualidad.

Un cumulo de estatus que normaliza la marcha de la actividad admite a maniobrar un privilegio para comprobar la entrada de requerimientos o sectores en ubicaciones tangible o en ordenadores (Henríquez, 2010). Para obtener un estatus que normalice con prioridad los objetivos de las tareas se requiere que tome con superioridad los controles de las conexiones que les asignan a los usuarios.

Admitir o impugnar la utilización de un bien tangible o eventual a usuarias u organismos, para otorgar luminosidad al propósito, se avisa para poner en funcionamiento la intervención de ingreso tangible, que está centrado en la admisión y partida a usuarias consentidas (Morales, 2012).

Para otorgar privilegios a departamentos autorizados por comités de la entidad se admite por el logro que ha llegado ser la necesidad de la misión del plan que se va implantar en la entidad.

Una posesión es fundamental en la erudición de la instrucción relacionado al tacto de facultar honor en los cibernautas para que efectué el desempeño que goza a cumplir (Dirección Nacional Seguridad y protección, 2019).

Basado al estudio enunciado es fundamental que el usuario tenga instrucción de los roles que debe cumplir cuando desempeñe sus funciones.

Indicadores

Compromiso con los colaboradores

El compromiso con los colaboradores logra ser un instrumento que se posee el individuo cuando se requiera llevar a examinar propósitos, cumplimiento y unión con los funcionarios en el punto de su labor (Rocha y Böhrt, 2004).

Para ejecutar nuestro estudio se requiere que los altos funcionarios y colaboradores lleven un vínculo laboral óptimo siendo este un medio para cumplir con el propósito de la entidad.

Medidas de Acceso

Las medidas de accesos apropiado de la información personal, se incorpora el acceso, la difusión, manejo, extracción, traslado, etc., de manera que esto es importante para confirmar la vida privada de las personas. De manera que, la relación con otros derechos humanos como la semejanza y no la marginación, siempre que descubren información privada se puede dar lugar al encierro de la persona (Marqueo, Moreno & Recio, 2017).

Nuestra investigación muestra que la vía más importante son las medidas que hay que tomar para proteger la información de nuestros usuarios, otorgándole el compromiso de que pueda acceder, consultar, siempre será una información confiable.

Inducción

La inducción en una pieza fundamental para lograr una variación didáctica y administrativa eficaz del servicio siendo notificado para adaptar el curso de transformación en la entidad (Artavia, Muñoz y Jiménez, 1999).

Para tener un mejor conocimiento e información de los temas que requiere una creación, desarrollo de modernos variaciones en las entidades se exige inducción a los funcionarios.

Subcategoría 3. Sistemas y Aplicaciones

Los sistemas y aplicaciones conforma los procedimientos de comprender los diversos progresos, ya que consiente a imaginar los distintos componentes, siendo convertidos, en las sucesiones que se obtiene en los efectos de la sucesión (Betancur, 2009).

En el estudio los sistemas y las aplicaciones es fundamental ya que es para acceder e modelar nuestra propuestas necesitamos de los accesos al sistemas y aplicaciones que tiene la financiera.

El curso que notifica lo puede dominar, siendo neutral en lo que solicita para adquirir posición en la que se extiende, entablando una partición en la indagación del cumulo de estatus que normaliza la marcha de la actividad (Dominguez, 2012).

En el estudio notificar los incidentes que observamos en el sistemas y aplicaciones es poder conocer los vulnerabilidades que podría estar en peligro los documentos e información de la financiera.

Los cumulo de estatus que normaliza la marcha de la actividad recolectan fases del interior, búsqueda, entre otros, ampliando la lealtad de los representantes con los que pacta la entidad al conceder una sencilla entrada al testimonio que requiere (Carrasco, 2015).

Para el estudio el sistema tiene que poner en marcha las fases, rangos, que requiere para que tengan reglas de seguridad y poder resguardar la información de la entidad.

Los sistemas y aplicaciones entabla con dispositivos que recauda, métodos, transferencias de los testimonios que requiere facultando el programa, estructura, manipulación y valoración de las asistencias (Santana, Tavares, Miranda, Custodio, Chaves y Oliveira, 2017).

Para elaborar un modelo en un sistema y aplicación se requiere ver que opciones va tener para ordenar sus funciones que obtendrá los colaboradores, siendo este primordial cuando acceda al sistema.

El reciente soporte más intenso y más ahorrador hace a las entidades a sugerir la extracción de sus datos o servicio que se establece en una reserva céntrico o un componente céntrico hacia novedosas propuestas (Rodríguez y Daureo, 2003).

Cuando se extrae información o data de sistemas y aplicaciones se requiere de mantener servidores de mantenimiento para restablecer los datos si no tienen los sistemas copia de seguridad.

Indicadores:

Uso

El uso se relaciona al modelo de las actividades a realizar efectuando la continuación de notas y documentos de la utilidad en un acción de la data y en el progresivo incremento en las asistencia virtuales que interceden con distintos tareas (Garrido, 2013). La acción de usar efectúa la ejecución de realizar tareas y modelos que queremos crear según las necesidades de los clientes y colaboradores.

Acceso

El acceso se presenta en la entrada a la norma compilado para que distintas cibernautas efectúen enriquecimiento en el resultado, siendo indispensable en las monumentales entidades que notifican la asistencia de la compilación de la configuración profunda de los principios que interceden en los ordenadores (Echevarría, 2014).

Para ejecutar o tener conectividad a una información se requiere los accesos a una fuente técnica que nos dé el privilegio de poder de entrar a las distintas puertas de conexión.

Monitoreo

El monitoreo se establece constantemente por tareas de inspección por contradictorios disposiciones que orientan a una guía, abarcando la ocupación de impedir eventos que ocasionen deterioros o circunstancias comprometidas al organismo desde la posición capitalista e individuo, conteniendo apreciaciones en las tareas que inspeccionan inusualmente (Vega y Nieve, 2016).

La propuesta es establecer automatización en los monitoreos que realiza la entidad para mejorar una destacada labor de los funcionarios.

Categorías Emergentes

Activos de Información

Los activos de información es un cotejo de accidentes que emplea un registro de los testimonios, componentes, antecedentes y usuarios que tiene la obligación de guiar e inspeccionar con principios la distribución de los escritos viendo el estado de reserva (Voutssas, 2010).

Los documentos o data que repercute la información de las entidades se tiene la obligación de evaluar y tener la reserva de custodiar para poner en estado los distintos documentos que tiene la organización.

La organización debe entender que las amenazas que pueden ser atacadas son los activos de información, siendo un gran reto para la entidad en tener siempre estrategias para alegar los ataques que vulneren su estabilidad, proponiendo una gran acción a tomar cuando ejecutan controles para evitar estas incidentes (De Freitas, 2008).

Los documentos, base de datos, reportes, sistemas, entre otros son fundamentales que requieran de protección ya que para la competencia en una gran amenaza, siendo estos atacados hasta vulnerar o hurtar estos recursos sustanciales por las entidades.

Los activos están compuestos por antecedentes que se relaciona con un propósito, siendo reservado acorde a medios de referencias (Vega, 2008). En nuestra investigación tenemos el alcance de observar que los activos de información se vinculan conforme a la exigencia del usuario.

En las entidades se resguarda en ubicaciones opuestos de la entidad interno e externo, los antecedentes, testimonios y data de la entidad en complejos ordenadores conectados a distintos mecanismos e instrumentos que reciba y tenga vínculos de conexión (Nahabetián, 2015). La data que tiene las entidades se reserva en ubicaciones que reguarden los registros de los usuarios, como en plataforma o sistemas que tienen acceso los colaboradores.

El desarrollo de mecanismos en el enlace vigente obliga a ejecutar un registro explayado a la dinámica que opera los testimonios para estandarizar los antecedentes a los mecanismos, unificando en grupos de incidentes usuales a los antecedentes vinculados en los modelos (Merchan y Gomez, 2011). En la investigación los activos de información se explayan en documentos, sistemas, entre otros, agrupándolos a través de cargos que tienen conexión con los sistemas.

Perfiles y Roles

Los perfiles y roles se desarrolla cuando se tiene establecido el rol del cargo, siendo esto importante para tener una conexión con el perfil que tiene en el sistema, identificando los roles que tendría el perfil, siendo los roles las opciones que tendría el colaborador en el momento que maneje el sistema (Zapata y Ceballos, 2010).

Para el desarrollo tener una conexión al ordenador o sistemas se requiere de un perfil vinculado al sistema, otorgando el perfil a un cargo que ha sido observado y evaluado para cubrir ciertas vinculaciones con otros sistemas.

Los perfiles y roles se abrevia por propiedades reiteradas en medio de la averiguación que compila en la inspección y se funda una figura del protagonista irreal, comprendiendo la cifra de rasgos que obtiene para el boceto en los instrumentos (Rodríguez, 2011).

Para llevar a cabo la investigación se debe conocer minuciosamente los perfiles y roles que se le asignan a cada individuo para el desarrollo de los prototipos o modelos empleados para la organización.

Para requerir un perfil y un rol se precisa de averiguación, a manera de propiedades que procedan con las pautas en el empleo de la averiguación, incluidas en las formas del cibernauta (Hernández, 1993). Para crear la estructura de los modelos o prototipos se requiere de estudio del perfil de individuo para emplear la conexión con el sistema de las entidades.

Para el perfil y rol se requiere de patrón que será empleado en las administración de capacidades, distinción en la línea de la función, la especificación de labores, métodos o tipos de cargo, concierna en beneficiosos para los aspirantes como el controlador (Sandoval, Montaño, Miguel y Ramos, 2012).

Para que los colaboradores tengan conectividad con los sistemas de la entidad se requiere de tener específicamente los cargos que ocupan siendo eso regularizado por un controlador.

Los perfiles establece variantes regentes en el plan de estudios, conglomerando las competencias, capacidades, pericia y postura que se entabla en su crecimiento, en aspecto formal según el experto en adiestramiento (Pirela, Prieto y Pulido, 2017).

La investigación para definir los perfiles y roles en el sistema y aplicaciones de la organización se requiere de que el usuario que va asumir sus responsabilidades posea destreza, experiencia en su función para asegurar un grato conducción en el sistema de la entidad.

2.4 Empresa

2.4.1 Descripción de la empresa

La financiera Credinka se forma a nivel nacional por necesidad de otorgar productos financieros accesibles y confiables a las personas emprendedoras para mejorar la calidad de vida de sus hijos y familia. Comenzó en el país como una caja rural siendo el gran paso al sector financiero, la sede principal estaba en la Región del Cusco, y luego se expandió a nivel nacional.

Visión:

“Ser una de las principales instituciones financieras líder en micro finanzas en el Perú”.

Misión:

“Creces, Crecemos”.

CONSULTA RUC: 20328178070 - FINANCIERA CREDINKA S.A. - CREDINKA S.A.			
Número de RUC:	20328178070 - FINANCIERA CREDINKA S.A. - CREDINKA S.A.		
Tipo Contribuyente:	SOCIEDAD ANONIMA		
Nombre Comercial:	CREDINKA S.A.		
Fecha de Inscripción:	05/03/1997	**Fecha Inicio de Actividades:**	01/04/1997
Estado del Contribuyente:	ACTIVO		
Condición del Contribuyente:	HABIDO		
Dirección del Domicilio Fiscal:	MZA. J LOTE. 8 URB. QUISPICANCHIS (TORRE CREDINKA MED CDRA PUENT MARCAVALLE) CUSCO - CUSCO - CUSCO		
Sistema de Emisión de Comprobante:	MANUAL/COMPUTARIZADO	**Actividad de Comercio Exterior:**	SIN ACTIVIDAD
Sistema de Contabilidad:	COMPUTARIZADO		
Actividad(es) Económica(s):	Principal - 6499 - OTRAS ACTIVIDADES DE SERVICIOS FINANCIEROS, EXCEPTO LAS DE SEGUROS Y FONDOS DE PENSIONES, N.C.P.		
Comprobantes de Pago c/aut. de impresión (F. 806 u 816):	FACTURA NOTA DE CREDITO GUIA DE REMISION - REMITENTE COMPROBANTE DE RETENCION		
Sistema de Emisión Electrónica:	DESDE LOS SISTEMAS DEL CONTRIBUYENTE. AUTORIZ DESDE 01/06/2018		
Afiliado al PLE desde:	01/01/2013		
Padrones :	Excluido del Régimen de Agentes de Retención de IGV a partir del 01/11/2012		

Figura 1. Registro de Financiera Credinka. *Fuente:* Sunat

2.4.2 Actividad económica de la empresa

En 2007, Credinka se incorpora al Grupo Financiero Diviso, siendo un gran apoyo económico para el crecimiento del sector financiero y económico a nivel nacional. También existe dentro del Grupo Diviso; Diviso Fondos y Diviso bolsa.

En DIVISO Fondos, es un comité donde se maneja activos de administrativos con un capital de US$ 75 millones, además ofrece a sus clientes fondos mutuos y fondos para que inviertan en el sector inmobiliario. También en DIVISO Bolsa, es un grupo administrado con cerca de US$ 400 millones de activos bajo al mando del grupo financiero, otorga beneficios ofrece de Intermediación Bursátil, Gestión de Patrimonios y Finanzas Corporativas.

El grupo Financiero, está registrada en la Bolsa de Valores de Lima, con el código “DIVIC1” desde 2007, administra un capital de US$700 MM., tiene una gran participación como accionista en la Bolsa de Valores de Lima, siendo representado por directorio de la financiera y está implicado en la Bolsa de Productos de Chile.

El grupo Diviso es auditado por la SBS (Superintendencia de Banca Seguros) y AFP, acorde a la ley de Supervisión Consolidada y por la SMV (Superintendencia del Mercado de Valores). La financiera está conformada por los altos directores y la protección y resguardo en el mercado nacional, cuenta con un gran equipo profesional que tiene más de veinte años en el rubro financiero y mercado de capitales.

2.4.3 Información económica y financiera de la empresa

La financiera Credinka, siendo ahora parte del grupo Diviso, se extiende en el mercado por el amplio experiencia y capital que administra por más de US$ 900 millones de dólares y ahora con la confianza que precede sus 133,000 clientes a nivel nacional.

También como parte del grupo, tiene como accionista el Fondo de Inversión DMP del gobierno de Dinamarca, el fondo le otorga un gran apoyo en las actividad económicas, por ser un país que tiene mercados emergentes en micro finanzas y ACCION GATEWAY FUND, es un líder accionario en micro finanzas , que cuenta con una gran experiencia en la industria financiera peruana, siendo su objetivo el crecimiento en las zonas rurales del país y en la posibilidad de llevar a los clientes a un sistema financiero más formal.

ACCIONISTAS	ACCIONES	VALOR NOMINAL	CAPITAL	PARTICIPACIÓN
DIVISO GRUPO FINANCIERO S.A.	125,583,641	S/.1.00	S/ 125,583,641	82.34%
DANISH MICROFINANCE PARTNERS K/S	12,574,903	S/.1.00	S/ 12,574,903	8.24%
ACCION Gateway Fund, LLC	12,574,903	S/.1.00	S/ 12,574,903	8.24%
Otros	1,784,710	S/.1.00	S/ 1,784,710	1.17%
Total	152,518,157	S/.1.00	S/ 152,518,157	100.00%

Figura 2. Estructura Accionaria de la Financiera Credinka. *Fuente:* Financiera Credinka S.A

2.4.5 Proyectos Actuales

Nuestro plan actual que tiene la financiera Credinka, es seguir expandiendo nuestros servicios bajo la necesidad de los clientes que lo requieren, ya que ofrecemos bajos tasas de interés en el momento que nuestro clientes piden un crédito.

Este año se lanzó nuestro seguro Soat contra accidentes y daños vehiculares, que beneficia a nuestros clientes por las bajas tasas de interés que ofrecemos.

2.4.6 Perspectiva empresarial

Ser la primera entidad financiera a nivel nacional con productos que beneficien a agricultores y a usuarios que tengan pequeña y mediana empresa. También Credinka tiene el propósito de seguir creciendo en el sector financiero hasta formarnos como entidad bancaria.

CAPITULO III

MÉTODO

3.1 Tipo, nivel y método

Sintagma

En la investigación el sintagma son distintos maneras de formular las estructuras de exploración, instruido por figurativos que detalla prototipo o pautas que escalonan gradualmente sucesiones que busca designar progresivamente un elemento a un modo total (Hurtado, 2010).

Nuestro estudio es sintagma holística a manera que nos proporciona la exploración de tipos, bosquejos o prototipos que permita mejorar y enriquecer de manera gradual con la investigación.

Enfoque

El Enfoque es de tipo mixto.

Se define que el enfoque son herramientas que recaudan datos no normalizados. La recaudación de datos consiste en lograr los objetivos y las ideas que fueron reevaluados por los usuarios (Hernández, 2014).

Las herramientas que nos va otorgar el apoyo de recolectar la información de los clientes, siendo una gran ayuda para cumplir los objetivos de nuestra división.

Tipo

El tipo de nuestra investigación es proyectivo.

El tipo de modelo investiga específica los dominios principales de las personas, equipos, corporación u otra rareza que es sometido al análisis. En una instrucción descriptiva se escoge una colección de cuestiones y evalúa cada una de ellas deliberadamente, para explicar lo que investiga. El modelo de preparación nos puede otorgar un nivel de pronóstico (Cauas, 2015).

En la investigación el tipo de estudio nos va a otorgar el medio para medir el modelo o boceto que vamos a seguir para determinar una buena herramienta de solución.

Nivel

Se define nivel como una cota de búsqueda que refiere una categoría de profundidad que lleva a aproximarse a una rareza o elemento de enseñanza (Gallardo 2017).

En definitiva en nuestra investigación los niveles nos van a otorgar datos que podemos calificar a nivel de rangos, fases, para poder determinar un mejor objetivo en nuestra investigación. Siendo nuestra estudio comprensivo.

Método

Se define método como una actividad usual a todas las ciencias, de manera que se trata de métodos inflexible formulado lógicamente, que deja conseguir un grupo de instrucciones en un modo sistemático y organizado (Maya, 2014).

En la investigación los métodos son procedimientos lógicos que vamos a seguir, para llevar a cabo las herramientas que se va utilizar en nuestra investigación.

La argumentación deductiva e inductiva es primordial para el análisis del estudio. Permitiendo la deducción el consentimiento de acceder un enlace de series y exploración que admita a proceder a través de probabilidades pieza de sugerencias. Para la inducción implica aglomerar sabiduría e indagación recluido (Davila, 2006). En nuestra investigación el método deductivo e inductivo son primordiales, permitiendo el deductivo en entablar entre nuestra información y probabilidades un vínculo de recomendaciones para eliminar las vulnerabilidades, y el inductivo un medio para distinguir las experiencias con la información encontrada.

3.2 Categoría y subcategorías apriorísticas

Tabla 1

Matriz de clasificación de las categorías y subcategorías

Categorías
Gestión de Control de Accesos
Subcategorías apriorísticas
Políticas de Accesos
Control de Accesos
Accesos al sistema y aplicaciones

Fuente: Elaboración Propia.

3.3 Población, muestra y unidades informantes

Población

Se define población como un grupo de herramientas que tienes ciertas peculiaridades que se puede evaluar. Por ese motivo la población y muestra se califica como inductivo, siendo que la parte examinada sea objetiva de la realidad, para que se asegure formas en el resultado que se recogió en la investigación (Lopez, 2004).

La población es una herramienta fundamental para analizar el estudio que nos va determinar a una gran proporción de personas que vamos a evaluar durante el proceso de nuestra investigación.

La población que va a intervenir durante el proceso de la investigación es la división de riesgos de la entidad financiera, perteneciendo al área de seguridad de información, riesgo operacional y continuidad de negocios, constituido por jefes, analistas y colaboradores, haciendo un total de 41 colaboradores.

Tabla 2

Matriz del Personal de la Entidad Financiera

	Área Seguridad de Información	Área Riesgo Operacional y Continuidad de Negocios	Total
Jefe	1	1	2
Colaboradores	10	18	28
Analistas	10	20	30
Total	21	39	60

Fuente: Elaboración Propia.

Muestra

La muestra se define en dos modelos: probabilística y no probabilística, son métodos de muestreo probabilísticos, que nos servirán como modelo de la probabilidad que tiene cada usuario en la evaluación para ser incorporado a través de una elección aleatoria. Con las técnicas de muestreo de carácter no probabilístico, la elección del estudio es examinada por ciertas definiciones, pautas, entre otros (Otzen & Manterola, 2017).

En definitiva, la investigación es la muestra que gran parte representa la población, donde vamos a evaluar y analizar el proceso de verificación para llevar a cabo una solución a los problemas.

La muestra va estar por 18 colaboradores, 2 jefes y 10 analistas siendo trabajadores en el área de seguridad de información, y riesgo operacional y continuidad de negocio, el total de 30 trabajadores, siendo esta información nuestra muestra de estudio.

Unidades Informativas

Es un grupo de tareas que a partir de la recolección de datos, promueve a la presentación de los resultados que están en los gráficos y tablas. La información se recoge a través de encuestas o evaluaciones que nos puede otorgar un resultado eficaz (Bustamante, 2017).

En la investigación la medida de recolectar datos a través de cuestionario o evaluación, puede otorgarnos rápidos resultados que nos podrá ayudar a un determinado grupo de colaboradores. Las unidades informativas que vamos a usar para obtener la recolección de datos son a través hojas de encuestas.

3.4 Técnicas e instrumentos

Técnicas

Las técnicas se caracterizan por estar como herramientas sistemáticas, en un análisis cuantitativo y cualitativo. De esta manera la evaluación va tener medidas de evaluación, para tener un buen significado a través de sus objetivos y de su alcance de término horizontal (Roble & Aviles, 2016). En nuestra investigación las técnicas nos van apoyar como medio de herramientas que van hacer un buen uso de seleccionar mejor nuestros objetivos, propósito que debemos implementar en nuestro plan de investigación.

Durante el proceso de recolección de datos hacia los colaboradores, se va manejar la técnica de encuesta, siendo el instrumento el cuestionario. También, la técnica entrevista, siendo el instrumento la ficha de entrevista.

Instrumentos

Los instrumentos son recolección de datos cualitativos, que nos permite diferenciar diversas métodos y capacidades para la recogida de nuestra información, definiendo muestra teóricas y herramientas comunes que nos puede ayudar para aplicar las técnicas más importantes para la recogida de los datos, que han sido halladas a través de entrevistas y nube de ideas (Izcara, 2014). En definitiva, los instrumentos es una parte fundamental para evaluar las técnicas de evaluación para llevar a un determinado método, que vamos a ejecutar durante la implementación de la solución.

Validez

La herramienta es evaluado a través del personal de la investigación, para evaluar y dar la conformidad, que los datos que van a medir y validar nuestros indicadores y objetivos de nuestra investigación. (Cabrera, Londoño & Bello, 2008).

En nuestra investigación la palabra validez es un significado que confirma que la información y datos que utilizamos son altamente confiables y claros durante los procesos de la investigación.

Tabla 3

Validación de especialistas

Nro.	Nombre del especialista	Especialidad	Grado	Criterio
1	Chavez Alvarado, Walter Amador	Educación	Mg.	Aplicable
2	Fox Cortez, Julio Alonso	Educación	Dr.	Aplicable
3	Ramos Muñoz, Alfredo Marino	Tecnología de Información	Mg.	Aplicable

Fuente: Elaboración Propia.

Confiabilidad

Cuando se usa una herramienta que ha cambiado los instrumentos, no nos confía la seguridad y confianza de las herramientas originales, siendo este medio para establecer una confianza en el momento de aprobar, evaluar los datos de la investigación (Mendoza & Garza, 2009).

En la investigación la confiabilidad se verifica a través de la evaluación de los datos que vamos a presentar en la investigación, reflejando que los datos que están en nuestro trabajo sean primordialmente validados a través de herramientas estadísticos. Para tener confiabilidad en los instrumentos que hemos estado utilizando para obtener los resultados de la investigación, se efectuó el Alfa de Cronbach.

Tabla 4

Confiabilidad en el instrumento

Alfa de Cronbach	N° de ítems
,725	20

Fuente: Elaboración Propia.

3.5 Procedimientos

Se realizó los siguientes pasos, para llevar a cabo nuestra investigación:

Paso 1: Selección del tema y de la entidad que se va investigar.

Paso 2: Tener claro los objetivos que se va cumplir durante el proceso del estudio.

Paso 3: Definir las teorías que se va seguir para llevar a cabo nuestra investigación.

Paso 4: Identificar antecedentes referentes a nuestra investigación.

Paso 5: Definir si el muestreo va ser aleatorio o por conveniencia.

Paso 6: Buscar las categorías problema, las subcategorías y los indicadores

Paso 7: Formular las preguntas para el cuestionario y la entrevista

Paso 8: Realizar el vaciado de las entrevistas y el cuestionario

Paso 9: Utilizar el programa Atlas. Ti para el análisis de los datos de la entrevista y el cuestionario

Paso 10: Realizar en el programa la triangulación mixta, con los análisis de la entrevista y el cuestionario.

Paso 11: Realizar el Pareto, identificamos los problemas primordiales según los sustentos de los encuestados.

Paso 12: Identificar los problemas de la financiera, señalar los objetivos de la propuesta.

Paso 13: Identificar los productos para llevar a cabo la solución de los problemas.

Paso 14: Realizar los ingresos y egresos que tiene que realizar la financiera.

Paso 15: Señalar la conclusión y sugerencias.

3.6 Análisis de datos

El diseño para la metodología del siguiente trabajo es Proyectiva. Se determinó proyectiva ya que nuestro trabajo de investigación depende de un plan que referencie un problema, objetivos, para llegar a la solución de las necesidades que tiene una organización del sector económico o bancario.

Cuantitativo

El método cuantitativo se asigna de elementos de una variables en una población de usuarios o clientes, que estudia con unidades básicas, en la muestra y en la herramientas se trabaja con números.

Los números o individuos son agarrados totalmente por una gran categoría de abstracción (Canales, 2006).

En la investigación el método nos otorgara una gran variante de beneficios para recolectar datos o información de determinados grupo de individuos.

Cualitativo

El método cualitativo destaca por elementos que se implementan en las herramientas y procedimientos cualitativos, los cuales los datos son complicados de descubrir o de localizar por diferentes procesos y realidades difíciles de alcanzar, por ser muy poco encontrados (Mora, 2002).

En definitiva el método cualitativo es la recolección de datos que se determina a través de actividades naturales que vamos a observar durante el transcursos de agrupas las respuestas a nuestra solución.

Mixto

La determinación de mixto es un modelo de estudio que se evalúa con norma de investigación. El método que orienta en la recolección, evaluación y modificación de datos, se va llevar a diferentes fases de procesos cualitativos y cuantitativos en una investigación o lista de conocimientos (Díaz, 2014).

El modelo mixto es un método donde se combina el modelo cuantitativo y cualitativo, orientándose a varias rangos de calificación para el análisis y recolección de datos.

CAPITULO IV
RESULTADOS y DISCUSIÓN

4.1 Descripción de resultados

En la categoría gestión de control de acceso se definió tres subcategorías las cuales fueron políticas de acceso, control de acceso y sistemas y aplicaciones, dentro de las subcategorías se definió indicadores, en la cual se propuso ítems, para medir la en base a los indicadores las subcategorías, para poder identificar el valor del problema de la financiera, con los valores nunca, a veces, normalmente, casi siempre y siempre que se determinó cuando se realizó el cuestionario. De tal modo, se desarrolló el diagrama de Pareto, donde se identificó tres problemas críticos, de la subcategoría política de acceso y sistemas y aplicaciones, para poder llevar a cabo a una solución.

4.2. Categoría Gestión de Control de Acceso

Tabla 5

Frecuencias y porcentajes de los ítems correspondientes a la sub categoría Políticas de Acceso

Ítem	Nunca		A veces		Normalmente		Casi siempre		Siempre	
	f	%	f	%	f	%	f	%	f	%
1. ¿Cuándo un trabajador comienza a elaborar y asumir sus funciones se le otorgan sus respectivos usuarios al sistema de la financiera?	1	3%	4	13%	14	47%	5	17%	6	20%
2. ¿Solicita permisos para ingresar a información secreta, confidencial e interna que no tiene que ver con su cargo?	11	37%	4	13%	3	10%	8	27%	4	13%
3. ¿Los colaboradores cumplen con los controles de acceso de seguridad cuando manejan la información de los clientes?	7	23%	10	33%	10	33%	10	33%	1	3%
4. ¿Considera Ud. que la financiera cumple con las políticas de seguridad de información para salvaguardar la información	0	0%	8	27%	10	33%	12	40%	0	0%
5. ¿Considera Ud. que los accesos que se le otorgan a los colaboradores tengan restricciones de seguridad?	8	27%	6	20%	9	30%	10	33%	4	13%

6. ¿Que la información que usas tienen controles de seguridad en los sistemas y aplicaciones de la empresa?	0	0%	7	23%	8	27%	9	30%	6	20%
7. ¿Cuándo se le otorga acceso a los jefes y los proveedores crees que se le debe restringir los accesos que no están a su cargo?	5	17%	8	27%	7	23%	3	10%	11	37%

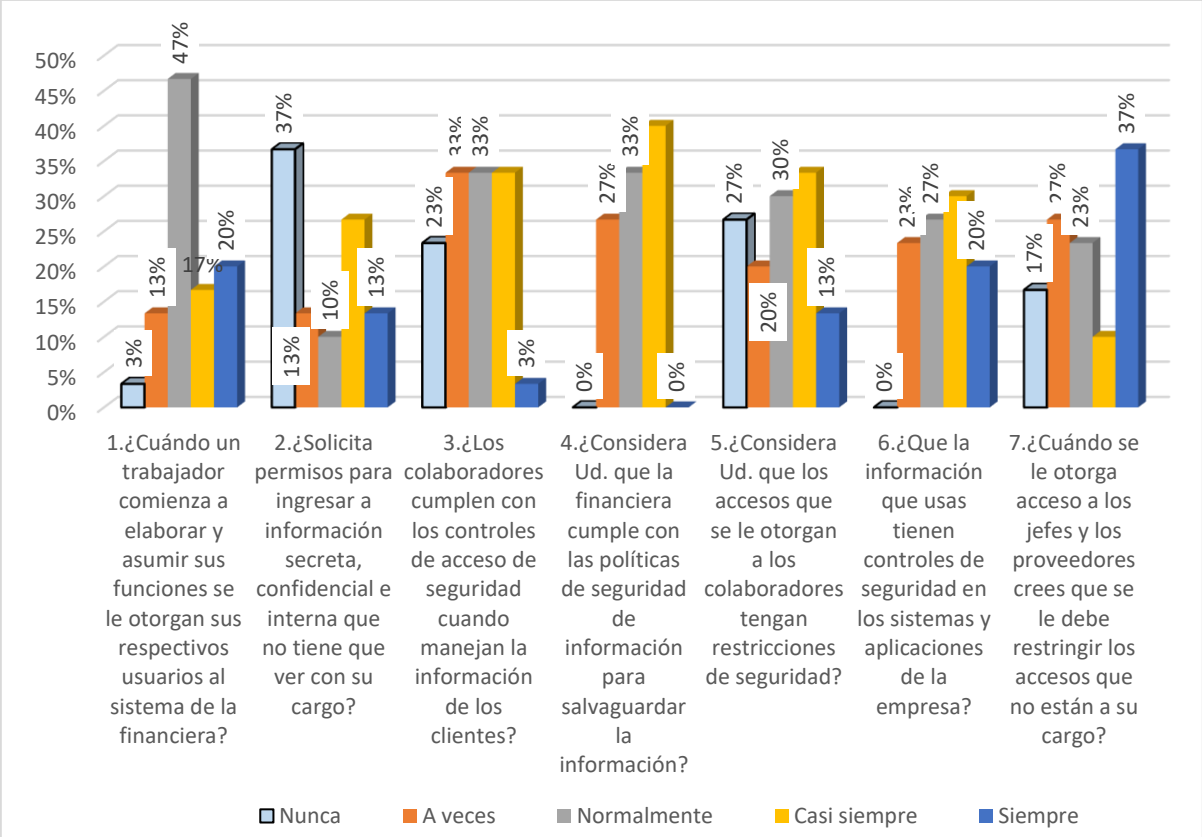


Figura 3. Frecuencias y porcentajes de los ítems correspondientes a la sub categoría Políticas de Acceso

En tabla 5 y en la figura 3 se muestra los ítems de la subcategoría políticas de acceso, del cuestionario realizado a 30 colaboradores de la financiera se obtuvo como resultado, del ítems 1 se observar que el 47% de los colaboradores, piensa que un trabajador comienza a elaborar y asumir sus funciones normalmente cuando se le otorgan sus respectivos usuarios al sistema de la financiera, sin embargo el 3% manifestaron que nunca se les otorgan sus respectivos usuarios al sistema de la financiera.

En el ítem 2 se observar que el 37% de los colaboradores nunca solicitan permisos para ingresar a información secreta, confidencial e interna que no tiene que ver con su cargo, de manera que el 27% casi siempre solicitan permisos para obtener alguna información secreta, confidencial e interna que no tiene que ver con su cargo. En el ítem 3 podemos ver que el 33% de los colaboradores cumplen con los controles de acceso de seguridad entre a veces, normalmente y casi siempre manejan la información de los clientes, mientras el 3% siempre cumplen con los controles de acceso de seguridad.

En el ítem 4 el 40% de los colaboradores opina que la financiera cumple casi siempre con las políticas de seguridad de información para salvaguardar la información, sin embargo hay un 27% que a veces cumple con las políticas de seguridad de información. En el ítem 5 el 33% de los colaboradores indicaron que los accesos que se le otorgan a los colaboradores casi siempre tengan restricciones de seguridad, mientras el 13% siempre tienen acceso son sus respectivas restricciones de seguridad.

En el ítem 6 el 30% de los colaboradores piensa que la información que usa tiene casi siempre controles de seguridad en los sistemas y aplicaciones de la empresa, mientras el 23% a veces tiene controles de seguridad en la información que usa. En el ítem 7 el 37% manifiesta que los colaboradores cuando se le otorga acceso a los jefes y los proveedores creen que siempre se le debe restringir los accesos que no están a su cargo, de manera que el 17% nunca se le restrieguen los accesos a los jefe y a los proveedores que no están a su cargo.

Tabla 6

Frecuencias y porcentajes de los ítems correspondientes a la sub categoría Control de accesos

Ítem	Nunca		A veces		Normalmente		Casi siempre		Siempre	
	f	%	f	%	f	%	f	%	f	%
8. ¿Ha recibido alguna documentación donde se comprometa a usar con responsabilidad la información que maneja y usa en el sistema de la empresa?	4	13%	2	7%	8	27%	8	27%	7	23%

9. ¿Los proveedores cuando inician un contrato con la financiera firman un contrato de confiabilidad?	1	3%	2	7%	6	20%	11	37%	10	33%
10. ¿Cuándo se le otorga acceso a los colaboradores se requiere de alguna conformidad del jefe o gerente encargado?	1	3%	0	0%	13	43%	6	20%	10	33%
11. ¿Cuándo comparten documentos confidenciales a proveedores o a la SBS, se requiere de conformidad del jefe o gerente?	4	13%	4	13%	13	43%	11	37%	4	13%
12. ¿Ha recibido inducción sobre el manejo de la información cuando accede al sistema de la empresa?	0	0%	4	13%	7	23%	11	37%	8	27%
13. ¿Considera Ud. que se debería orientar a los colaboradores acerca de las responsabilidades que tiene el usuario cuando usa información de la empresa?	0	0%	0	0%	6	20%	11	37%	13	43%

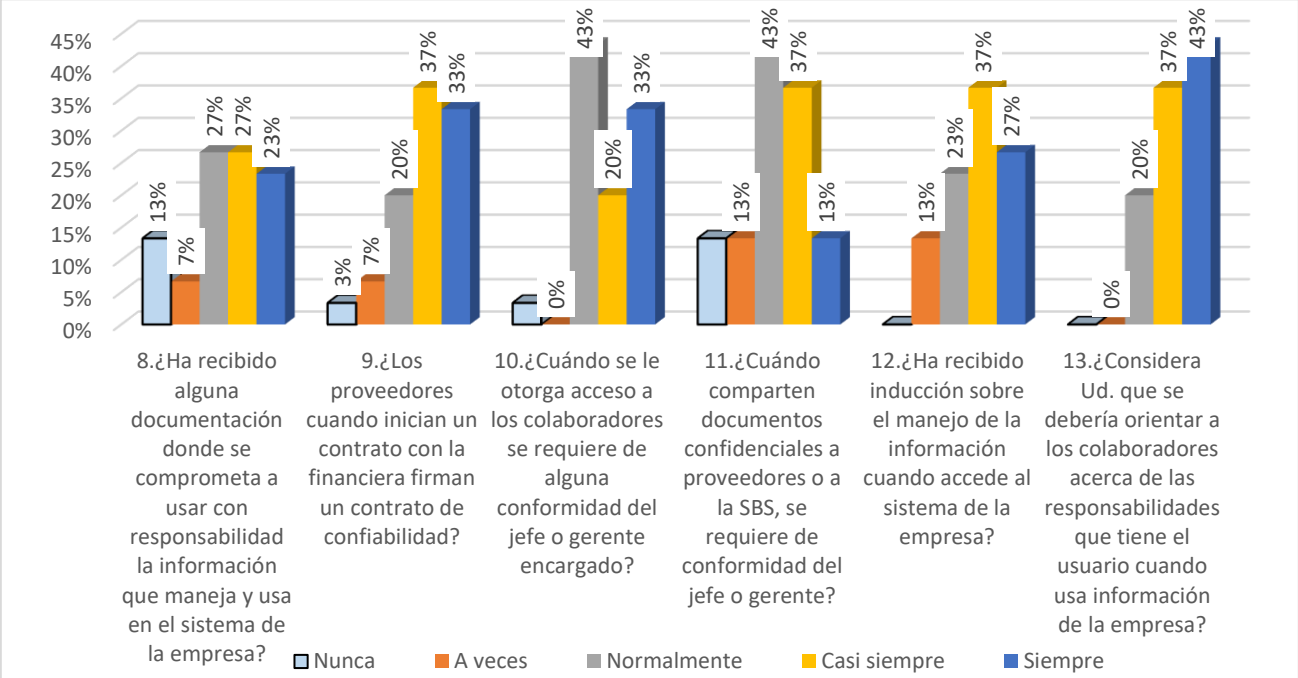


Figura 4. Frecuencias y porcentajes de los ítems correspondientes a la sub categoría Control de Acceso.

En tabla 6 y en la figura 4 se muestra los ítems de la subcategoría control de acceso, del cuestionario realizado a 30 colaboradores de la financiera se obtuvo como resultado, en el ítems 8 el 27% de los colaboradores opina que ha recibido normalmente y casi siempre alguna documentación donde se comprometa a usar con responsabilidad la información que maneja y usa en el sistema de la empresa, mientras el 7% a veces ha recibido alguna documentación.

En el ítem 9 el 37%, los colaboradores opina que los proveedores cuando inician un contrato con la financiera casi siempre firman un contrato de confiabilidad, sin embargo el 3% manifiesta que los proveedores nunca han firmado un contrato cuando comienza a elaborar. En el ítem 10 el 43% de los colaboradores opina que cuando se le otorga acceso a los colaboradores se requiere normalmente de alguna conformidad del jefe o gerente encargado, mientras el 3% nunca se requiere de conformidad cuando se le otorga sus accesos.

En el ítem 11 el 43% de los colaboradores opina que cuando comparten documentos confidenciales a proveedores o a la SBS, se requiere normalmente de conformidad del jefe o gerente, sin embargo el 13% entre nunca, a veces y siempre requiere de conformidad del jefe o gerente cuando comparten documentos. En el ítem 12 el 37%, los colaboradores opina que casi siempre ha recibido inducción sobre el manejo de la información cuando accede al sistema de la empresa, mientras el 13% a veces ha recibido inducción y en el ítem 13 el 43% de los colaboradores considera que siempre se debería orientar a los colaboradores acerca de las responsabilidades que tiene el usuario cuando usa información de la empresa, y el 20% respondió que normalmente se debe orientar a los colaboradores.

Tabla 7

Frecuencias y porcentajes de los ítems correspondientes a la sub categoría Sistemas y Aplicaciones

Ítem	Nunca		Casi Nunca		A veces		Casi siempre		Siempre	
	f	%	f	%	f	%	f	%	f	%
14. ¿Todos los sistemas que usa el colaborador tienen definidos los roles y perfiles según los cargos que tiene?	4	13%	15	50%	8	27%	11	37%	3	10%
15. ¿Los sistemas que manejan los colaboradores tienen un usuario clave y contraseña?	0	0%	1	3%	13	43%	9	30%	7	23%
16. ¿Considera Ud. Que los controles no automatizados que tienen la empresa son de utilidad para verificar los accesos indebidos?	1	3%	9	30%	10	33%	9	30%	1	3%
17. ¿Para obtener accesos a los sistemas y aplicaciones que no están asignados según mi cargo, se requiere de la autorización de mi jefe o gerente?	1	3%	5	17%	12	40%	11	37%	7	23%

18. ¿Se realiza un adecuado monitoreo de los accesos que se le otorgan a los colaboradores de la empresa?	4	13%	9	30%	9	30%	12	40%	1	3%
19. ¿Ha observado ciertas irregularidades en el momento que los colaboradores usen la información de los clientes?	1	3%	9	30%	10	33%	7	23%	6	20%
20. ¿Recibe la empresa un informe diariamente?	0	0%	0	0%	17	57%	5	17%	2	7%

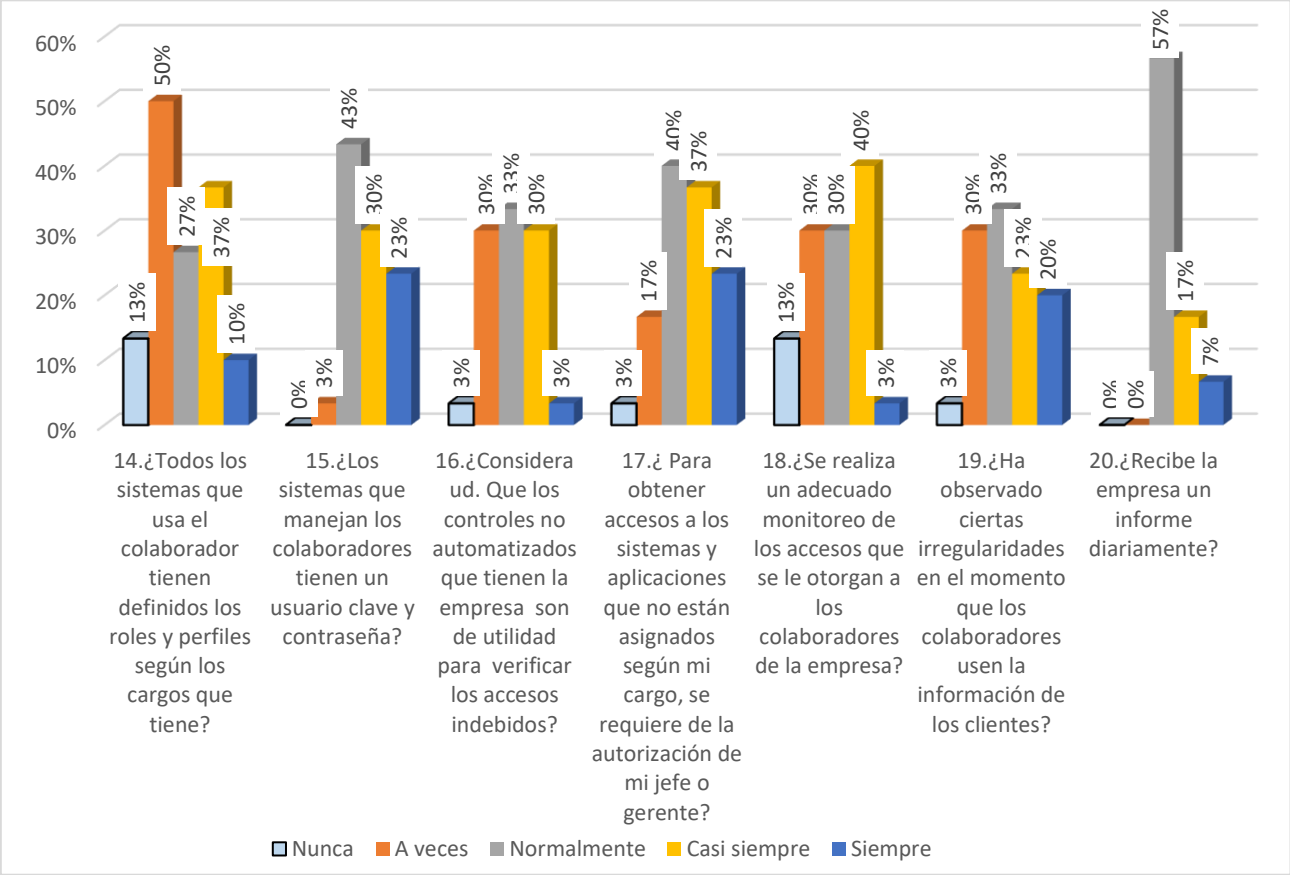


Figura 5. Frecuencias y porcentajes de los ítems correspondientes a la sub categoría Sistemas y Aplicaciones

En tabla 7 y en la figura 5 se muestra los ítems de la subcategoría control de acceso, del cuestionario realizado a 30 colaboradores de la financiera se obtuvo como resultado, en el ítems 14 el 50% de colaboradores opina que todos los sistemas que usa el colaborador tienen a veces definidos los roles y perfiles según los cargos que tiene, mientras que el 10% de los sistemas siempre tiene definidos los roles y perfiles.

En el ítem 15 el mayor porcentaje representa el 43% de los colaboradores que opina que los sistemas que manejan los colaboradores tienen normalmente un usuario clave y contraseña, sin embargo el 23% responde que los sistemas siempre tiene un usuario clave y contraseña en los sistemas que maneja. En el ítem 16 el 33% de los colaboradores considera normalmente que los controles no automatizados que tienen la empresa son de utilidad para verificar los accesos indebidos, sin embargo el 3% considera entre nunca y siempre que los controles no automatizados son de utilidad para la empresa.

En el ítem 17 se refleja que el 40% de los colaboradores piensa que para obtener accesos a los sistemas y aplicaciones que no están asignados según mi cargo, normalmente se requiere de la autorización de mi jefe o gerente, mientras el 3% nunca responde que nunca se requiere de autorización.

En el ítem 8 el 40% de los colaboradores piensa que casi siempre se realiza un adecuado monitoreo de los accesos que se le otorgan a los colaboradores de la empresa, sin embargo el 13% respondió que nunca se realiza monitoreo de los accesos. En el ítem 19 el 33% ha observado normalmente ciertas irregularidades en el momento que los colaboradores usen la información de los clientes, mientras que el 3% nunca ha observado irregularidades cuando los colaboradores usan información y en el ítem 20 el 57% responde que normalmente la empresa recibe un informe diariamente de los monitoreo, mientras que el 7% manifiesta que siempre recibe un informe.

Tabla 8

Pareto de la categoría control de accesos de una financiera, Lima, 2019

Ítem	Puntaje	%	Acumulativo	20.00%
3. ¿Los colaboradores cumplen con los controles de acceso de seguridad cuando manejan la información de los clientes?	27	7.65%	7.65%	20%
14. ¿Todos los sistemas que usa el colaborador tienen definidos los roles y perfiles según los cargos que tiene?	27	7.65%	15.30%	20%
5. ¿Considera Ud. que los accesos que se le otorgan a los colaboradores tengan restricciones de seguridad?	23	6.52%	21.81%	20%

18. ¿Se realiza un adecuado monitoreo de los accesos que se le otorgan a los colaboradores de la empresa?	22	6.23%	28.05%	20%
11. ¿Cuándo comparten documentos confidenciales a proveedores o a la SBS, se requiere de conformidad del jefe o gerente?	21	5.95%	33.99%	20%
7. ¿Cuándo se le otorga acceso a los jefes y los proveedores crees que se le debe restringir los accesos que no están a su cargo?	20	5.67%	39.66%	20%
16. ¿Considera Ud. Que los controles no automatizados que tienen la empresa son de utilidad para verificar los accesos indebidos?	20	5.67%	45.33%	20%
19. ¿Ha observado ciertas irregularidades en el momento que los colaboradores usen la información de los clientes?	20	5.67%	50.99%	20%
1. ¿Cuándo un trabajador comienza a elaborar y asumir sus funciones se le otorgan sus respectivos usuarios al sistema de la financiera?	19	5.38%	56.37%	20%
2. ¿Solicita permisos para ingresar a información secreta, confidencial e interna que no tiene que ver con su cargo?	18	5.10%	61.47%	20%
4. ¿Considera Ud. que la financiera cumple con las políticas de seguridad de información para salvaguardar la información?	18	5.10%	66.57%	20%
17. ¿Para obtener accesos a los sistemas y aplicaciones que no están asignados según mi cargo, se requiere de la autorización de mi jefe o gerente?	18	5.10%	71.67%	20%
20. ¿Recibe la empresa un informe diariamente?	17	4.82%	76.49%	20%
6. ¿Que la información que usas tienen controles de seguridad en los sistemas y aplicaciones de la empresa?	15	4.25%	80.74%	20%
8. ¿Ha recibido alguna documentación donde se comprometa a usar con responsabilidad la información que maneja y usa en el sistema de la empresa?	14	3.97%	84.70%	20%
10. ¿Cuándo se le otorga acceso a los colaboradores se requiere de alguna conformidad del jefe o gerente encargado?	14	3.97%	88.67%	20%
15. ¿Los sistemas que manejan los colaboradores tienen un usuario clave y contraseña?	14	3.97%	92.63%	20%
12. ¿Ha recibido inducción sobre el manejo de la información cuando accede al sistema de la empresa?	11	3.12%	95.75%	20%
9. ¿Los proveedores cuando inician un contrato con la financiera firman un contrato de confiabilidad?	9	2.55%	98.30%	20%
13. ¿Considera Ud. que se debería orientar a los colaboradores acerca de las responsabilidades que tiene el usuario cuando usa información de la empresa?	6	1.70%	100.00%	20%

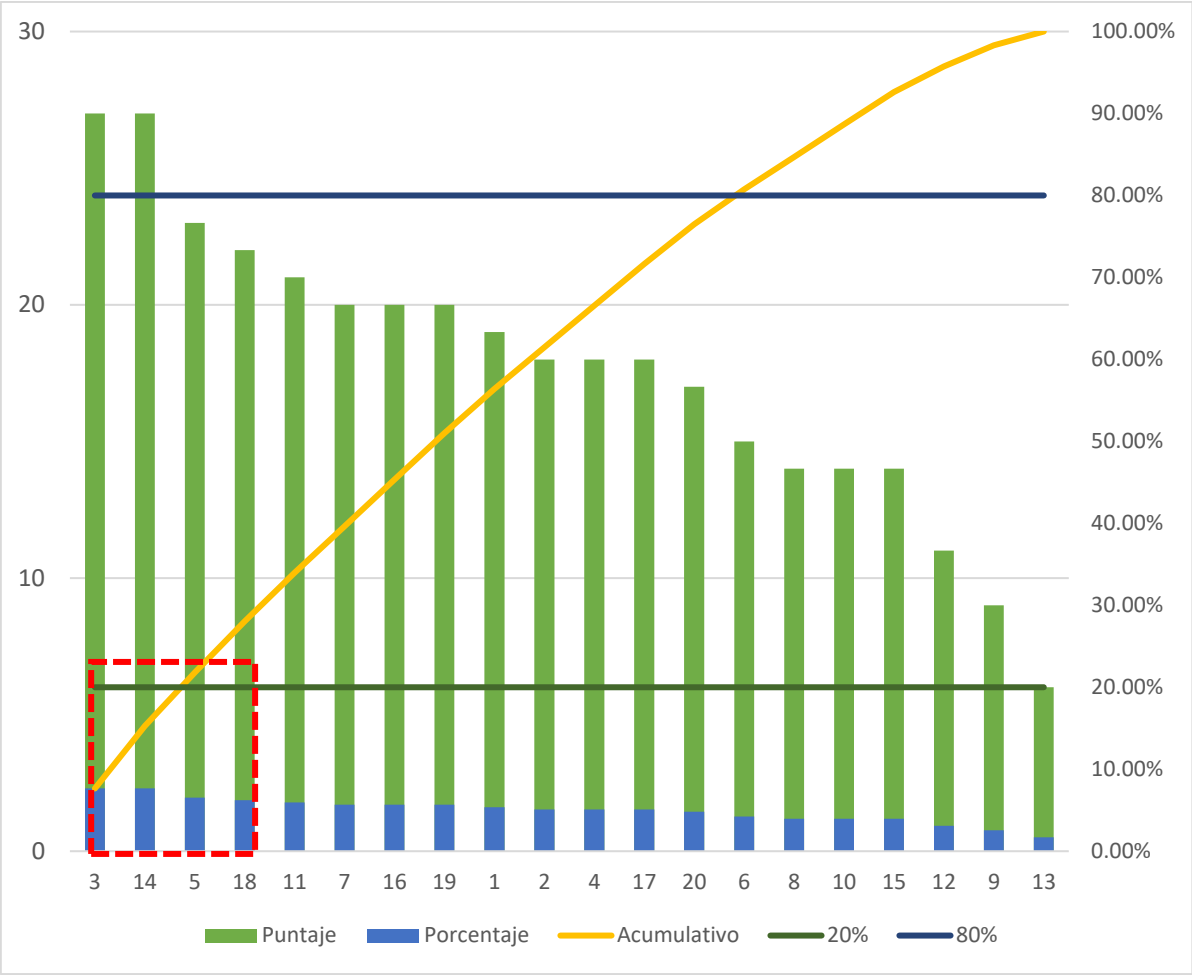


Figura 6. Pareto de la categoría gestión de control de accesos de una financiera, Lima, 2019

En la figura 6 y el tabla 8 muestra las 20 ítems que fue planteadas para realizar el cuestionario a los colaboradores de la financiera, en el momento de reunir los datos se observaron tres ítems críticas que realza el problema que está ocurriendo en la financiera, para plantear una solución. El ítem 3 siendo crítico, se considera ya que podría existir una gran dificulta cuando los colaboradores manejan la información de los clientes ya que se manifiesta que no cumplen con los controles de acceso de seguridad, en el ítem 14. Se refleja que los sistemas que usa el colaborador no tienen muy definidos sus roles y perfiles en el sistema que usa en la financiera, ya que puede acceder a más información que no le corresponde a su cargo y en el ítem 5, se refleja que no todos los accesos que se le otorgan a los colaboradores tengan restricciones de seguridad, manifestándose un problema referente a la divulgación de información que se maneja solo en la financiera.

Análisis cualitativo

Análisis de la subcategoría políticas de accesos

A nivel de respuesta de los entrevistados mencionaron que hay un proceso que sigue RR. HH, para solicitar los accesos a los colaboradores, según la política de la financiera los jefes del área deben seguir unos pasos para definir los accesos a los colaboradores, donde se menciona que tienen que estar con las conformidades respectivas del jefe del área.

Otro factor relacionado a la subcategoría, según los entrevistado manifestaron que para que los colaboradores cumplan con las políticas de seguridad, la financiera realiza difusiones y capacitaciones, pero aun así los colaboradores no cumplen con las políticas siendo una gran dificultad para la empresa, en el momento que se le otorgan al colaborador sus accesos no podemos tener un control en el momento que usa la información, ya que se ha visto que los colaboradores pueden compartir su usuario o contraseña a diferentes colaboradores, para avanzar con su labores. También los entrevistados nos mencionaron que el área de seguridad de información controla los accesos a través de la matriz de perfiles según al cargo, donde está definido el perfil para el proveedor y para los colaboradores, pero no se cuenta con medidas de accesos para poder determinar las restricciones y que activos de información van a tener el colaborador y el proveedor cuando acceden al sistema.

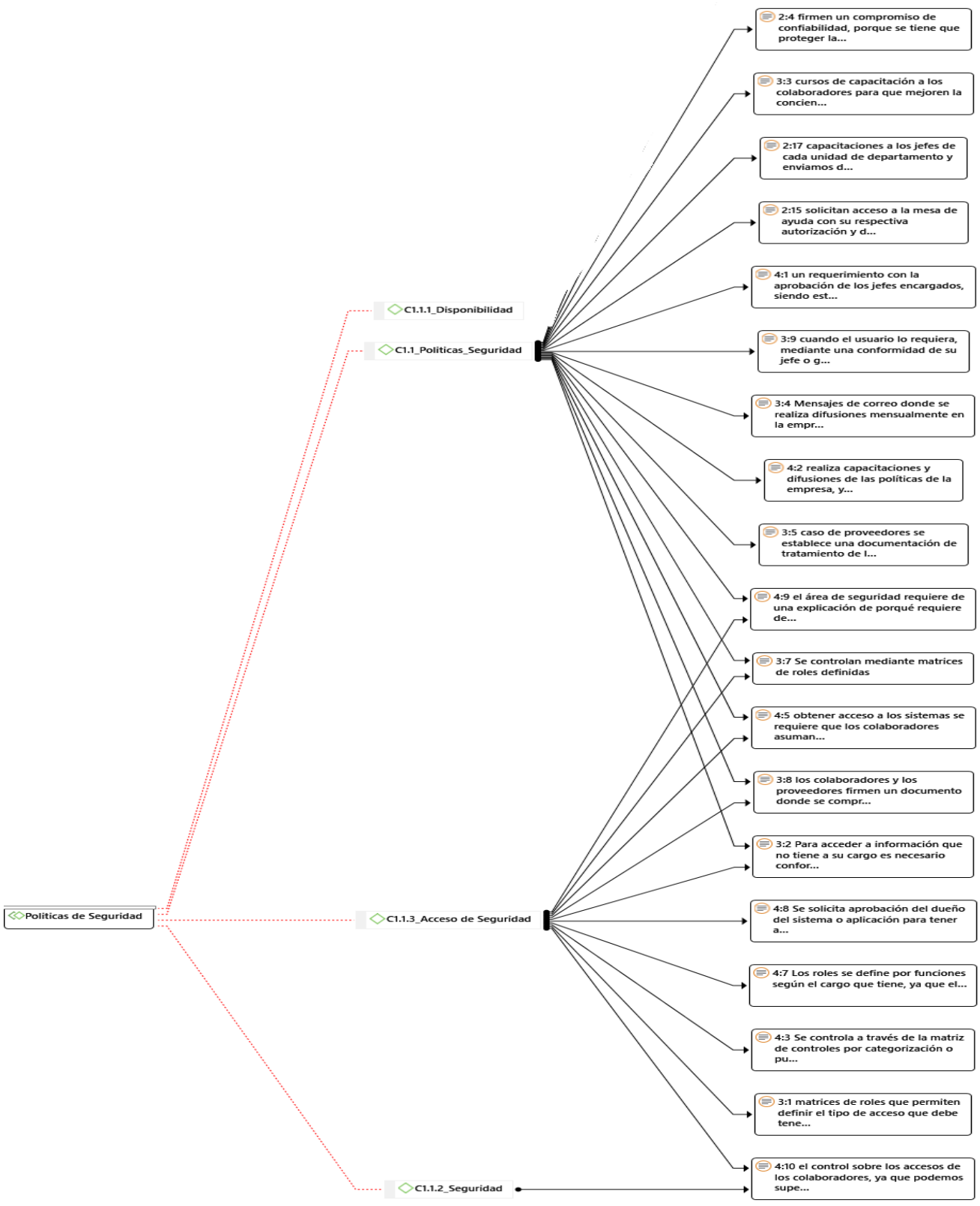


Figura 7. Análisis de la subcategoría políticas de accesos

Fuente: Elaboración Propia.

Análisis de la subcategoría control de acceso

Según los tres entrevistados mencionaron que los proveedores y los colaboradores firman un documento de confiabilidad siendo este documento como un compromiso que tiene el colaborador y el proveedor con la empresa. Así mismo, los entrevistados manifestaron que orientan a los colaboradores por difusiones, que se envía mensualmente por un correo general a todos los colaboradores, sobre temas de seguridad de información, activos de información, escritorio limpio, etc., también se capacita a los colaboradores y a los jefes por área, sobre temas de la circular G-140 de la SBS, PDP, etc.

En la política de la financiera y según el área de seguridad de información el colaborador para tener acceso a los sistemas se debe tener conformidad de los responsables o del dueño del sistema, de manera que los entrevistados manifestaron que siempre el colaborador como responsable de sus funciones debe pedir conformidad de los dueños de los sistemas o de los encargados del área que tiene acceso al sistema que quiere acceder, ya que el colaborador va usar y manejar la información de otra área.

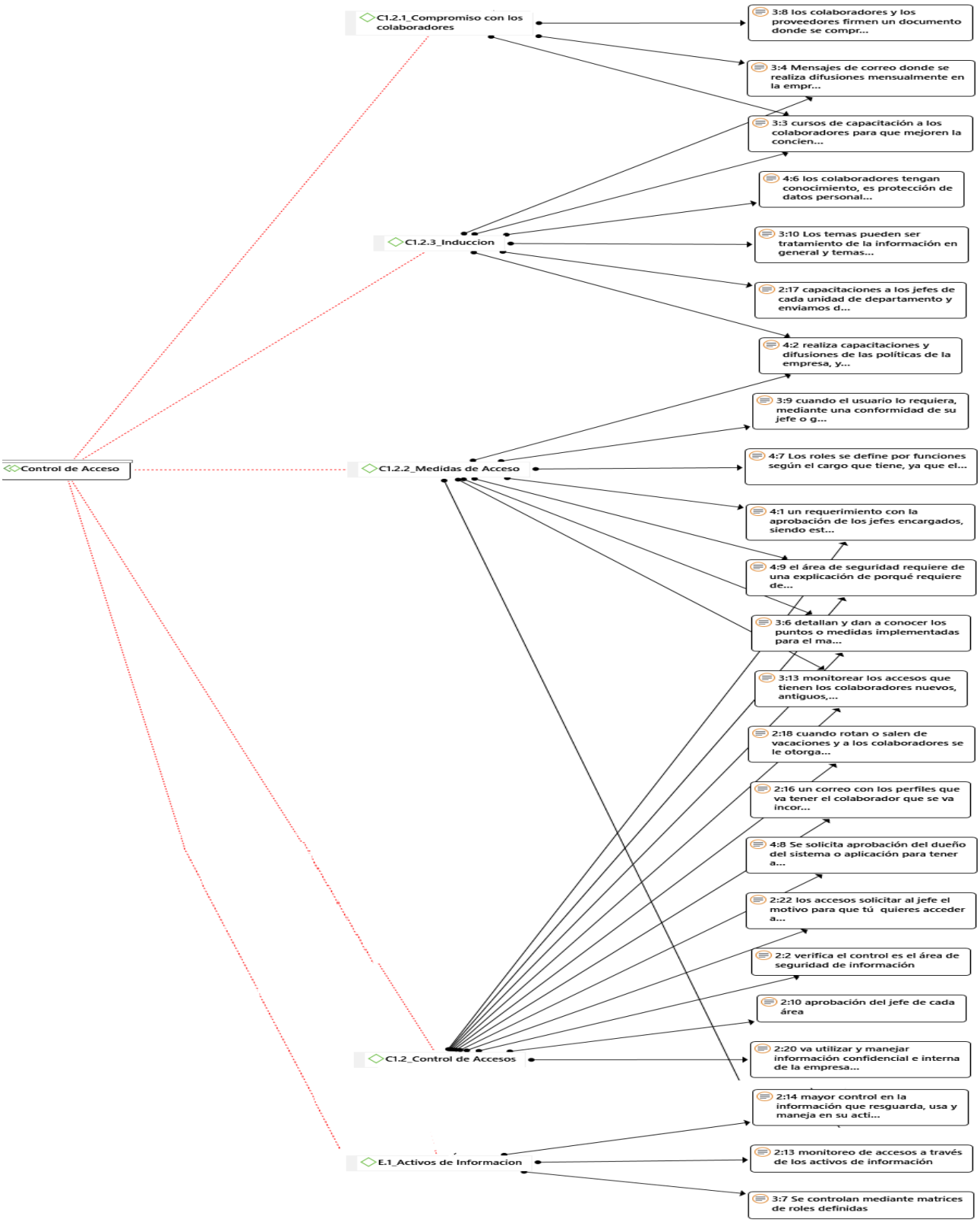


Figura 8. Análisis de la subcategoría control de accesos

Fuente: Elaboración Propia.

Análisis de la subcategoría sistemas y aplicaciones

Los entrevistados mencionaron que sería beneficioso si el área de seguridad de información usa herramientas nuevas cuando realiza un monitoreo de los sistemas y aplicaciones, ya que el área realiza monitoreo manuales, se podría ver si los colaboradores nuevos, antiguos, tendrían activos sus respectivos perfil en el sistema, y los cesados tienen bloqueado su accesos. Así mismo, el área de seguridad de información cuando realiza este monitoreo es muy dificultoso, ya que toma demasiado tiempo por la cantidad de colaboradores.

Los controles de accesos a los sistemas de la financiera es a través de un usuario y una contraseña, para acceder otro sistema el colaborador solicitante por correo solicitar al jefe el motivo para que tú quieres acceder ha dicho sistemas, para llevar a cabo dicho cambio se pide la conformidad de seguridad de información, con el tiempo establecido, y seguridad de información envía al área de TI o a mesa de ayuda.

Otro factor relacionado a la subcategoría, la definición del perfil se define con la aprobación del área que está solicitando el perfil, ya que esa área sabe que función va cumplir el cargo que se le va definir el perfil, el área de SI tiene una matriz de acceso basado a cargos para poder controlar los sistemas que debe tener cada perfil, pero este proceso no tiene un control ya que el jefe o el analista solicita cambios de perfil en el sistema evitando la conformidad de seguridad de información, ocasionando perdida de información cuando acceden al sistema, entre otros eventos, siendo estos eventos una gran pérdida de confianza que tiene el colaborador con la empresa.

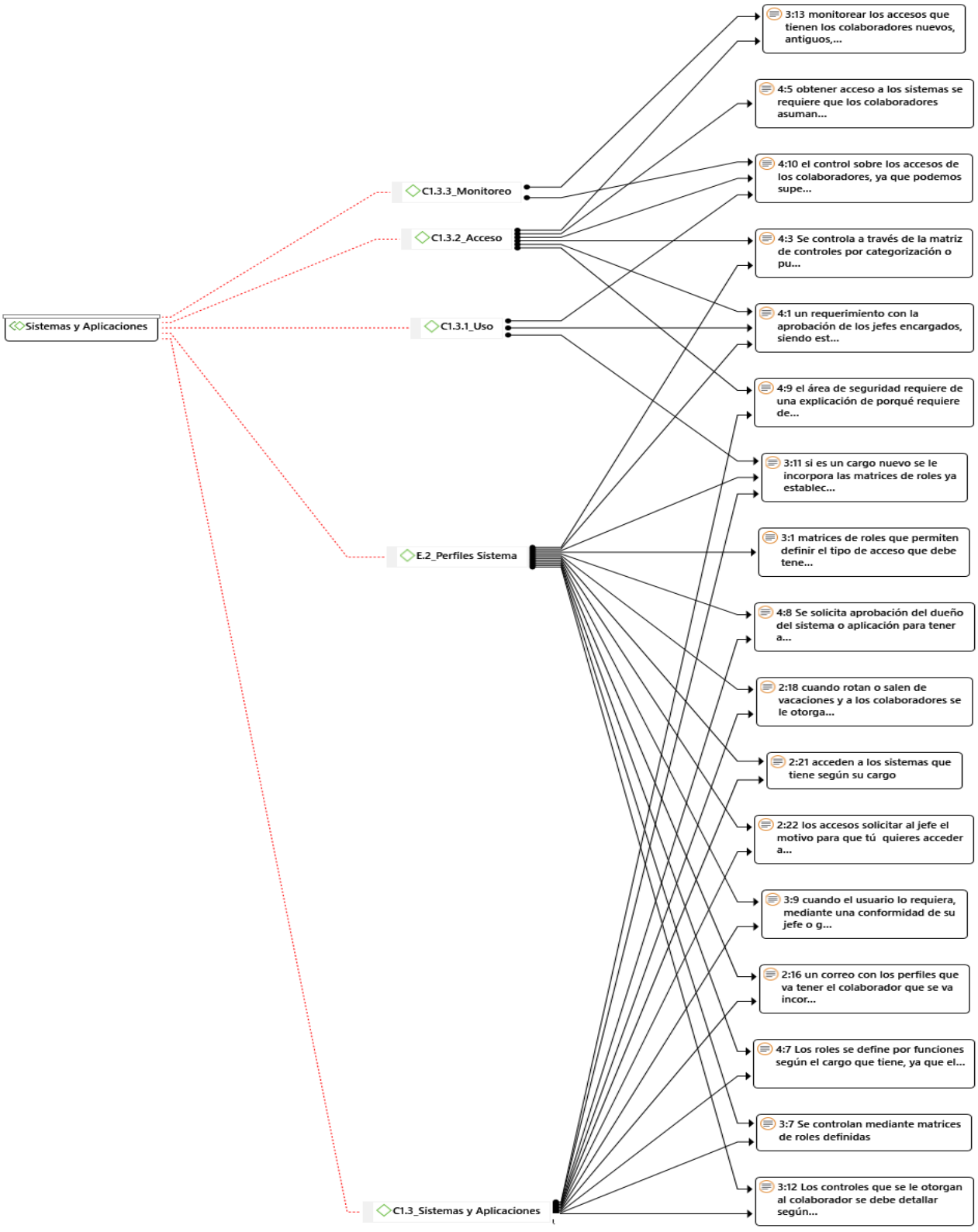


Figura 9. Análisis de la subcategoría sistemas y aplicaciones

Fuente: Elaboración Propia.

Diagnóstico Final

Según los resultados obtenidos de la encuesta que se realizó a 30 colaboradores de la financiera, con las entrevistas a 3 personas responsables en el área de seguridad de información de la misma financiera, para determinar el problemas que existe en la gestión de control de accesos se explica lo siguiente:

En la primera subcategoría políticas de acceso, el ítem 2 el 37% de los colaboradores nunca solicitan permisos para ingresar a información secreta, confidencial e interna que no tiene que ver con su cargo, sin embargo el 27% casi siempre solicita permisos para obtener alguna información secreta, confidencial e interna que no tiene que ver con su cargo. En el cual se comparó con el análisis de entrevista donde se recalca que hay un proceso donde RR.HH y seguridad de información solicita conformidades respectivas de los jefes de área para poder acceder a información, el 37% puede ser considerado que los gerentes o personas externas que solicitan de manera directa al área de TI, si dar conocimiento a área de Seguridad de información, por ser considerado un proceso muy lento en el momento que se espera la respuesta de seguridad de información, se puede observar que la posición del acceso a los sistemas para obtener la información no es muy considerado bajo los gerentes o jefe de departamento.

Así mismo, se evidencio que el ítem 3, el 33% de los colaboradores cumplen con los controles de acceso de seguridad entre a veces, normalmente y casi siempre manejan la información de los clientes, mientras el 3% siempre cumplen con los controles de acceso de seguridad. En el cual a relación con el análisis de la entrevista, los colaboradores para que cumplan con los controles y que la financiera cumpla con las políticas de seguridad, la financiera y el área de seguridad realiza difusiones y capacitaciones, pero aun así los colaboradores no cumplen con las políticas siendo una gran dificultad para la empresa, en el momento que acceden al sistema de la financiera, siendo una gran vulnerabilidad para la financiera.

Podemos ver que en el ítem 5, el 33% de los colaboradores indicaron que los accesos que se le otorgan a los colaboradores casi siempre tengan restricciones de seguridad, mientras el 13% siempre tienen acceso son sus respectivas restricciones de seguridad. En el cual a relación con el análisis de la entrevista, el área de seguridad controla los accesos a través matrices según al cargo, donde está definido el perfil para el proveedor y para los colaboradores, pero esto puede ser modificado por los jefes, así que parte de las políticas que existen en la financiera, de que la única autoridad para modificar o cambiar los accesos es el área de seguridad de información, pero algunas veces no es tomado consideración así que otras áreas pueden influenciar enviando sus listas de cargos, con sus respectivos accesos a los sistemas, perdiendo el área de seguridad de información el control de poder determinar qué medidas de accesos , que restricciones y que activos de información van a tener el colaborador y el proveedor cuando acceden al sistema.

También podemos ver que el ítem 10, el 43% de los colaboradores opina que cuando se le otorga acceso a los colaboradores se requiere normalmente de alguna conformidad del jefe o gerente encargado, mientras el 3% nunca se requiere de conformidad cuando se le otorga sus accesos y el ítem 11, el 43% de los colaboradores opina que cuando comparten documentos confidenciales a proveedores o a la SBS, se requiere normalmente de conformidad del jefe o gerente, sin embargo el 13% entre nunca, a veces y siempre requiere de conformidad del jefe o gerente cuando comparten documentos. En el cual a relación con el análisis de la entrevista, los colaboradores para pedir acceso y para compartir documentos, el área de seguridad de información para cualquier requerimiento se debe pedir primero conformidades del jefe del área solicitante, de manera que si el jefe no tiene conocimiento de que su compañero de trabajo está solicitando acceso al sistema, puede ocasionar una vulnerabilidad o un riesgo, por la disposición de la información, el proceso que sigue el área de seguridad de información, no es muy eficaz, ya que las demás áreas consideran que los únicos que deben tener autoridad para compartir sus documentos o dar acceso a sus colaboradores son ellos mismo, dando al área de seguridad de información una posición arriesgada, ya que no todos los colaboradores cumplen con el proceso.

En la tercera subcategoría sistemas y aplicaciones, podemos ver que el ítem 18, el 40% de los colaboradores piensa que casi siempre se realiza un adecuado monitoreo de los accesos que se le otorgan a los colaboradores de la empresa, sin embargo el 13% respondió que nunca se realiza monitoreo de los accesos y el ítem 16, el 33% de los colaboradores considera normalmente que los controles no automatizados que tienen la empresa son de utilidad para verificar los accesos indebidos, sin embargo el 3% considera que los controles no automatizados entre nunca y siempre son de utilidad para la empresa .En el cual a comparación con el análisis de la entrevista, sería beneficioso el adecuado uso de nuevas herramientas cuando realiza un monitoreo de los sistemas y aplicaciones, ya que como se realiza monitoreo no automatizado, podría ser un monitoreo muy dificultoso, ya que toma demasiado tiempo para identificar las observaciones, por eso la estrategia es automatizar los monitoreos, y tener la seguridad de que la información que nos envía el área de TI, es correcta, otorgándonos conocimiento de cuantas personas tienen acceso a los sistemas y aplicaciones de la financiera.

Además, visto que el ítem 14, el 50% de colaboradores opina que todos los sistemas que usa el colaborador tienen a veces definidos los roles y perfiles según los cargos que tiene, mientras que el 10% de los sistemas siempre tiene definidos los roles y perfiles. En el cual a comparación con el análisis de la entrevista, el perfil se define con la aprobación del área que está solicitando el perfil, pero el área de seguridad de información tiene una matriz de acceso basado a cargos para poder controlar los sistemas que debe tener cada perfil, pero este proceso no es muy eficaz, ya que el jefe de cualquier área puede realizar un cambio de perfil al colaborador sin el visto bueno de seguridad de información, ocasionando vulnerabilidades en la información cuando acceden al sistema sin autorización, siendo estos eventos una gran pérdida de confianza que tiene el colaborador con la empresa.

4.3 Propuesta

4.3.1 Fundamentos de la propuesta

En esta propuesta se presenta que la financiera requieren de modelos para la gestión de control de accesos, donde se pueda obtener una mejor manera de controlar a los riesgos de accesos inadecuados a la información que cuenta la financiera, se propone modelos para establecer en el área de seguridad de información cuando se designan funciones a los colaboradores con accesos a los sistemas que tiene la financiera, en líneas abajo se especifica las propuesta para lograr el objetivo de nuestra investigación.

4.3.2 Problemas

El estudio realizado se identificó tres problemas, basado a los incumplimientos de seguridad de información de los colaboradores cuando acceden a los sistemas de la financiera, tales como:

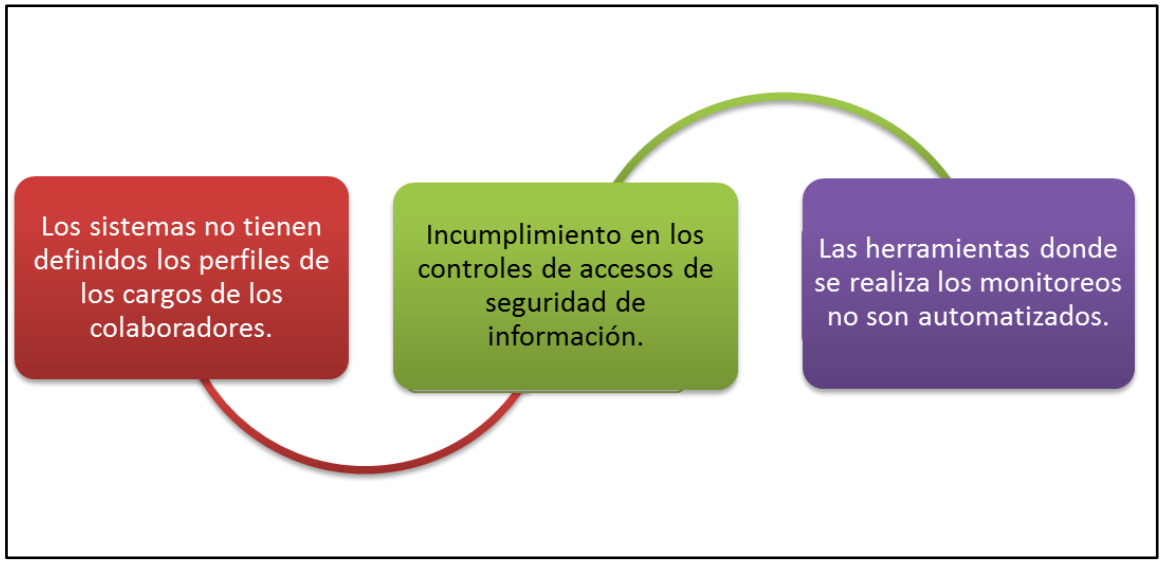


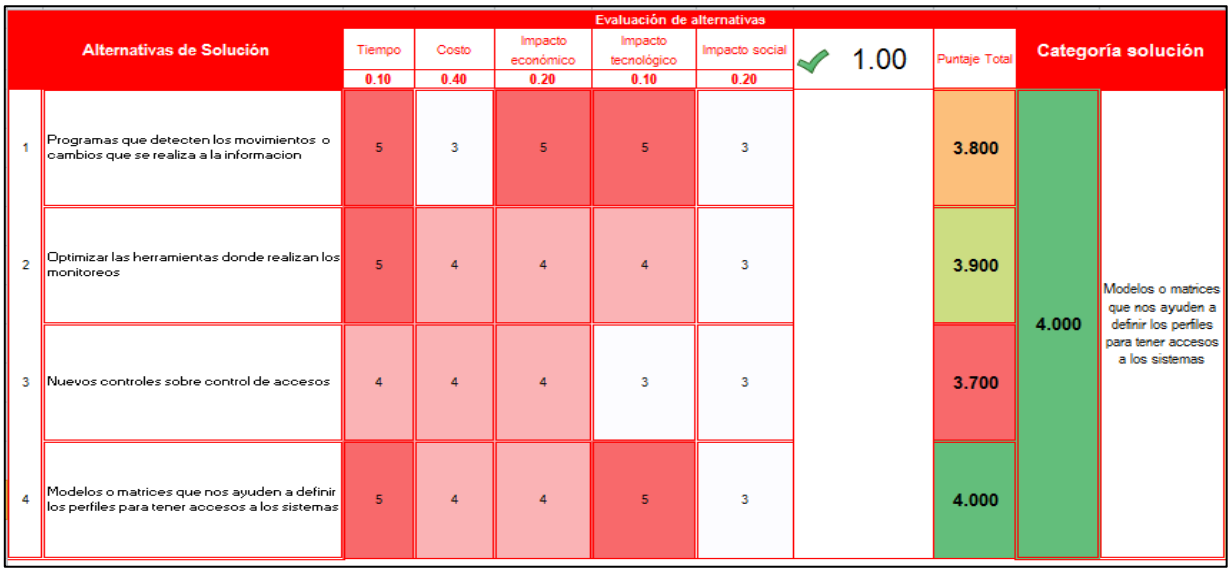
Figura 10. Priorización del problema de la financiera

Fuente: Elaboración Propia.

En la figura 10 presenta los problemas identificados a través de los análisis de las entrevistas y del cuestionario, para luego mostrar alternativas de soluciones a los objetivos propuestos.

4.3.3 Elección de la alternativa de solución

Para realizar el progreso de la gestión de control de acceso en la financiera, brindamos diferentes opciones de solución, y se ha considerado para la propuesta de solución de nuestro problema la categoría más alta, siendo esta opción para resolver la gestión de control de acceso, tales como se observa en la siguiente figura:



	Alternativas de Solución	Evaluación de alternativas							Categoría solución	
		Tiempo	Costo	Impacto económico	Impacto tecnológico	Impacto social	✔ 1.00	Puntaje Total		
		0.10	0.40	0.20	0.10	0.20				
1	Programas que detecten los movimientos o cambios que se realiza a la informacion	5	3	5	5	3		3.800	4.000	Modelos o matrices que nos ayuden a definir los perfiles para tener accesos a los sistemas
2	Optimizar las herramientas donde realizan los monitoreos	5	4	4	4	3		3.900		
3	Nuevos controles sobre control de accesos	4	4	4	3	3		3.700		
4	Modelos o matrices que nos ayuden a definir los perfiles para tener accesos a los sistemas	5	4	4	5	3		4.000		

Figura 11. Alternativas de solución. *Fuente:* Elaboración Propia.

Tabla 9

Criterios para la alternativa de solución

Rango/ Criterios	1	2	3	4	5
Tiempo	De 2h a más.	1h ½	1h.	½ h.	30min.
Costo	s/10.000 soles	s/5.000 soles	s/ 3.000 soles	s/1.000 soles	s/500.00 soles
Impacto Económico	Muy Alta perdida	Mayor Perdida	Perdida moderado	Menor perdida	Insignificante perdida
Impacto Tecnológico	Muy Insignificante	Insignificante	Favorable	Valioso	Muy Valioso
Impacto Social	Muy Bajo	Bajo	Moderado	Alto	Muy Alto

Fuente: Elaboración Propia.

4.3.4 Objetivos de la propuesta

Para disminuir los incumplimientos hacia la gestión de control de accesos y efectuar los objetivos hacia las alternativas de solución, se estableció tres objetivos:

Diseñar un modelo para definir los perfiles que van a interactuar con los accesos a los sistemas.

Proponer nuevos controles de accesos en los sistemas de información.

Elaborar un modelo que ayude optimizar la herramienta que usa el área de seguridad de información para realizar los monitoreos.

4.3.5 Justificación de la propuesta

En el trabajo de investigación se busca obtener nuevas formas de poder ayudar al área de seguridad de información, otorgándoles como propuesta modelos, controles para solucionar los problemas que pueden ser un riesgo para el área y para la financiera, siendo el área encargada de controlar, verificar y otorgar accesos a los colaboradores y a las personas externas.

Siendo estas herramientas como un medio de poder tener una buena comunicación con el área TI y RR.HH, ya que estas áreas buscan obtener un mejor proceso para los colaboradores y poder tener una mejor respuesta en la atención de los requerimientos, de manera que los inventarios sería una forma de poder obtener información más rápida de los sistemas y perfiles que tiene acceso los cargos de la financiera, y el inventario de los controles es una forma de poder tener un control en el momento que ocurre una incidencia o un evento de riesgo para la empresa.

Sin embargo, el modelo para los perfiles, va hacer una mejor forma de poder tener plasmado todos los cargos que tienen acceso a los diferentes sistemas de la financiera, y cuando ocurra un cambio de nombre, o quitar los accesos, el área de TI, va poder ver los cambio realizados por seguridad de información sin necesidad de enviar correos de confirmación o modificación. Cuando se realiza los monitoreos se podrá ver el tiempo, que se va realizar los monitoreos y las observaciones que tiene que sustentar el área de TI, otorgándoles a ellos un tiempo de espera.

4.3.6 Desarrollo de la propuesta

Objetivo 1: Diseñar un modelo para definir los perfiles que van a interactuar con los accesos a los sistemas.

Actividades:

En la tabla 10, se precisa las actividades que se va realizar para poder definir los perfiles en los sistemas, con los siguientes campos, Nro. de actividad, el nombre de la actividad, fecha de inicio y fin, el beneficio que nos va otorgar cada actividad y la persona responsable de cada actividad.

Tabla 10

Plan de actividades para la definición de los perfiles en los sistemas de la financiera, 2019.

Nro.	Actividad	Inicio	Días	Fin	Logro parcial	Responsable/s
1	Reunión con jefes de área	01/01/2020	1	02/01/2020	Transmisión de la construcción del modelo	Jefe de SI
2	Aprobación formal del modelo	03/01/2020	5	08/01/2020	Mejorar el proceso actual	Jefe de SI
3	Levantar los perfiles existentes	09/01/2020	20	29/01/2020	Información de los cargos actuales	Jefe de SI
4	Inventario de perfiles	30/01/2020	10	09/02/2020	Conocimiento de los perfiles existentes	Jefe de SI
5	Armado del modelo	10/02/2020	5	15/02/2020	Identificar los sistemas que van a tener acceso	Jefe de SI
6	Prueba piloto en el área de riesgos	16/02/2020	5	21/02/2020	Verificar de la efectividad del modelo	Jefe de SI
7	Corrección del modelo	22/02/2020	5	27/02/2020	Perfeccionar el modelo	Jefe de SI
8	Permiso de Gerencia General	28/02/2020	2	01/03/2020	Aprobación para la puesta en marcha	Gerente General
9	Ejecución	02/03/2020	5	07/03/2020	Mejorar el proceso	Jefe de SI

Fuente: Elaboración Propia.

También muestra en la tabla 10, las actividades con sus respectivas probabilidades que tenemos que seguir, si nos dificultad poder ejecutar las actividades definidas, cerrando así nuestro primer objetivo a realizar.

Tabla 11

Plan de actividades con sus respectivas posibilidades

Nro.	Actividad	Justificación
1	Reunión con jefes de área	Reunión con los Analista
2	Aprobación formal del modelo	Verificación para la aprobación
3	Levantar los perfiles existentes	Reporte de los perfiles que tienen los colaboradores activos
4	Inventario de perfiles	Lista de los perfiles de acorde al reporte
5	Armado del modelo	Creación de la estructura
6	Prueba piloto en el área de riesgos	Demo al área de riesgos
7	Corrección del modelo	Sugerencias del modelo
8	Permiso de Gerencia General	Permiso del gerente del área de riesgos
9	Ejecución	Demostración a todos los colaboradores

Fuente: Elaboración Propia.

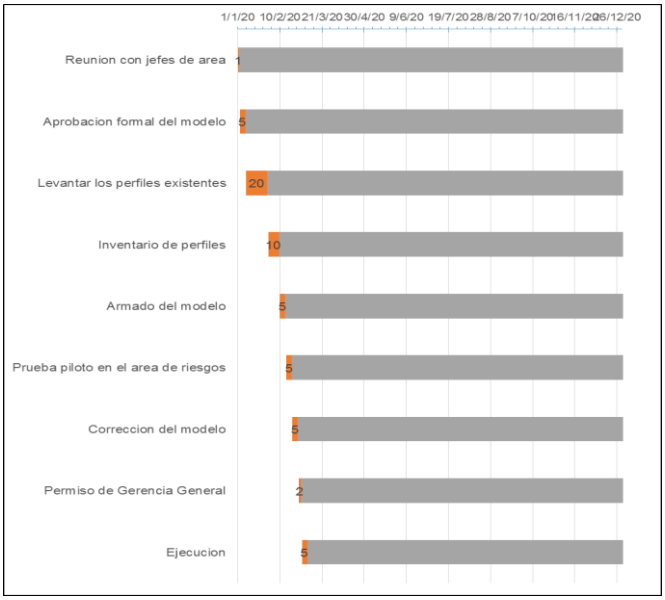


*Figura 12.*Plan de actividades para la definición de los perfiles. *Fuente:* Elaboración Propia.

En la figura 12 presenta los días de inicio que va realizar cada actividad hasta el último día de la ejecución.

Indicadores:

Para mostrar el primer objetivo, hemos puntualizado un adecuado indicador que nos muestre el interés propuesto.

Indicador 1:	**Indicador 2:**
$Cargo = \frac{Nº\ de\ perfiles\ que\ tienen\ cargo}{Total\ de\ Cargos} * 100$	$Perfiles = \frac{N°\ de\ cargos\ eliminados}{Total\ de\ perfiles\ bloqueados} * 100$

Cuadro 1. Indicadores para la definición de los perfiles en los sistemas de la financiera, 2019. *Fuente:* Elaboración Propia.

Los dos indicadores mostrados en el cuadro xx, el primer indicador nos presenta el número de perfiles que tiene cada cargo, con el total de cargos que tiene la financiera, multiplicado por cien. Podemos observar si los cargos que tienen su perfil, tienen el perfil que le corresponde.

También, en el segundo indicador, nos presenta el número de perfiles, bloqueados con el total de perfiles activos, multiplicado por cien. Podemos identificar si hay un buen manejo de bloqueo de perfiles en el momento que se elimina un cargo.

Ingresos y Egresos del Objetivo Nº1:

Tabla 12

Ingresos y egresos de Objetivo-1

Nro. De Actividades	Ingresos	Egresos	Utilidad/Pérdida
1	0.00	15.00	-15.00
2	0.00	15.00	-15.00
3	0.00	15.00	-15.00
4	0.00	499.99	-499.99
5	0.00	2267.00	-2267.00
6	0.00	0.00	0.00
7	0.00	1000.00	-1000.00
8	0.00	15.00	-15.00
9	0.00	0.00	0.00
Total	**0.00**	**S/ 3,826.99**	**-S/ 3,826.99**

Fuente: Elaboración Propia.

En la tabla 12 podemos ver los ingresos y egresos que han tenido todas las actividades, pero según el cuadro la financiera va tener un egreso de S/ 3,826.99 soles, en los siguientes cuadros se muestra los egresos que le corresponde a cada actividad:

Tabla 13

Egresos de las actividades 1, 2, 3 y 8

Egresos				
Código	**Descripción**	**Unidad**	**Cantidad**	**Total**
1	Hoja Bond	1	15	15
			Total	S/15.00

Fuente: Elaboración Propia

En la tabla 13 presenta los egresos de las actividades nº 1- Reunión con jefes de área nº2- Aprobación formal del modelo, nº3- Levantar los perfiles existentes y nº8- Permiso de Gerencia General, para ser el respectivo actividad usamos de papel hoja bond, para los informes que tenemos que presentar en el momento que se realiza una reunión, para el levantamiento de perfiles hay que presentar un informe y para solicitar el permiso del Gerente General hay que presentar una solicitud.

Tabla 14

Egresos de la actividad 4

Egresos				
Código	**Descripción**	**Unidad**	**Cantidad**	**Total**
1	Excel	1	499.99	499.99
			Total	S/499.99

Fuente: Elaboración Propia

En la tabla 14, evidencia el egreso de la actividad nº4 – Inventario de perfiles, para poder realizar esta actividad vamos a necesitar el programa Excel, si el responsable no tiene el programa en su pc.

Tabla 15

Egresos de la actividad 5

Egresos				
Código	**Descripción**	**Unidad**	**Cantidad**	**Total**
1	Compra de licencia de visual studio 2019	1	2,267.00	2,267.00
			Total	S/2,267.00

Fuente: Elaboración Propia.

En la tabla 15, indica que la actividad nº5- el armado del modelo, teniendo que comprar la licencia de visual studio 2019, para realizar el prototipo en esa plataforma.

Tabla 16

Egresos de la actividad 7

Egresos				
Código	**Descripción**	**Unidad**	**Cantidad**	**Total**
1	Profesional de apoyo	1	1000	1000
			Total	S/1,000.00

Fuente: Elaboración Propia.

En la tabla 16, nos indica que la actividad nº7- corrección del modelo, va tener un gasto de S/1,000.00 soles, ya que el personal de apoyo su salario va costar este monto.

Solución

Para solucion de nuestro objetivo, propusimos el modelo donde estan definidos los perfiles del sistema y el inventario donde podemos ver los perfiles de la financiera, la plantilla estaba en excel, basado a eso se realizo un modelo en la plataforma de visual studio, podemos encontrar los prototipos en el Anexo 2: Evidencias de la propuesta, donde podremos ver el modelo planteado, el primer prototipo es el login, donde el jefe de seguridad de información o el analista podra acceder a traves de su usuario y contraseña.

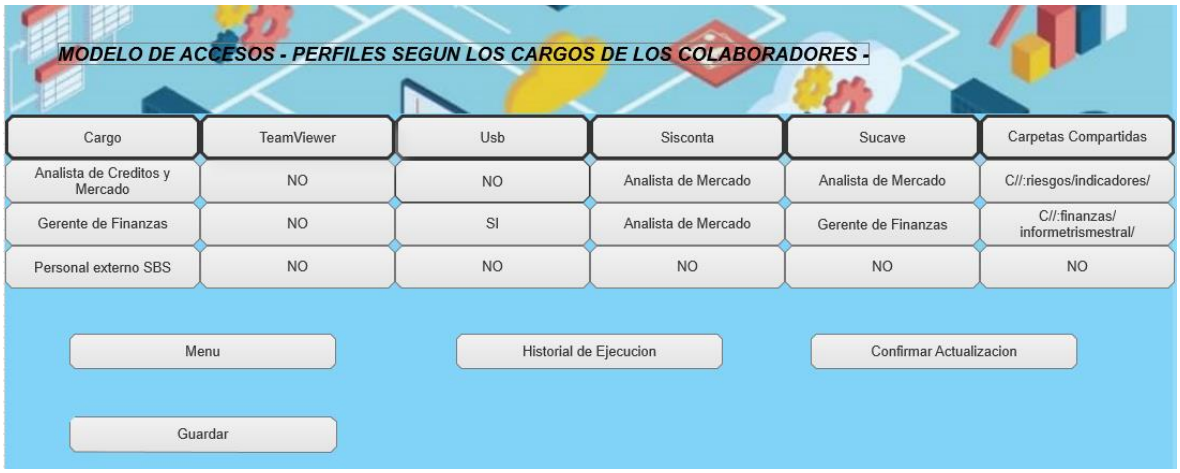


Figura 13. Prototipo de modelo de accesos y perfiles. *Fuente:* Elaboración propia.

Segunda prototipo, esta el menu, donde el usuario tendra la opcion de entrar a la matriz de perfiles, tambien podra acceder a los monitoreos y tendra la opcion de salir de la plataforma.

Tercer prototipo, entrando a la opcion de la matriz de perfiles, se refleja los campos que tiene que llenar el colaborador, los campos estan definidos por el; nº de cargo, el nombre del cargo, los sistemas que tiene la financiera como; el teamviewer, sisconta, el sucave, entre otros, tambien esta los accesos que tiene como; el usb y las carpetas compartidas que le corresponde segun su cargo, donde el jefe o el analista podra registrar los cargos como: Analista de Creditos y Mercado, Gerente de Finanzas y Personal Externo SBS,con sus respectivos perfiles y accesos que le corresponde, podemos observar que el personal externo no tiene acceso a ningun sistema o acceso, eso es debido a que como es personal externo debe solicitar al area de seguridad de información que le otorguen acceso a los sistemas que necesita con la conformidades de los jefe o gerentes de las areas que tienen acceso a los sistemas que quiere acceder. Tambien tiene la opcion de volver al menu.

Cuarta prototipo, podemos ver que el area de ti, ha recibido un aviso, de que no existe ningun en la matriz, de manera que ellos tienen la opcion de ejecutar el cambio, este aviso sucede cuando el analista o jefe de seguridad de información no ha realizado ningun cambio en el tercer plantilla, como el cambio de nombre del cargo, bloquear el acceso al usb, entre otros.

Quinta prototipo se comunicara al analista o al jefe de seguridad de información que se ha realizado la actualizacion de la matriz,teniendo la opcion de confirmar, que acepta el proceso realizado.

Sexta prototipo, podemos ver que en el registro que hemos realizado en la tercer plantilla, el analista cambia de nombre del perfil que tiene definido el cargo.

Septima prototipo, el area de TI, tendra el comunicado de que el area de seguridad de información ha realizado un cambio de nombre del perfil que tiene acceso al sistema que le corresponde segun el cargo, ejecutando el cambio al sistema.

Obtavo prototipo, el analista o jefe de seguridad de información podra ver que el cambio de perfil del sistema, se ha realizado,donde el area de seguridad de información esta confirmando que se ha realizado dicho cambio.

También se realizó el inventario de los perfiles existentes de la financiera, siendo una propuesta para tener un mayor control de los accesos que tiene el perfil, para la realización está considerado los siguientes campos: n° de perfiles, nombre del perfil, el área, el cargo que pertenece, los sistemas/ aplicaciones que tienen accesos y áreas primordiales, esa campo, es cuando sucede la pérdida del backup (copia de seguridad de la información), determinando si el perfil es primordial para el funcionamiento del negocio.

Objetivo 2: Proponer nuevos controles de accesos.

En la tabla 17, se precisa las actividades que se va realizar para poder definir los perfiles en los sistemas, con los siguientes campos, Nro. de actividad, el nombre de la actividad, fecha de inicio y fin, el beneficio que nos va otorgar cada actividad y la persona responsable de cada actividad. También nos muestra en la tabla 18, las actividades con sus respectivas probabilidades que tenemos que seguir, si nos dificultad poder ejecutar las actividades definidas, cerrando así nuestro primer objetivo a realizar.

Actividades:

Tabla 17

Plan de actividades para los nuevos controles de accesos en los sistemas de la financiera, 2019.

Nro.	Actividad	Inicio	Días	Fin	Logro parcial	Responsable/s
1	Reunión con los Jefe de Continuidad de Negocio	01/01/2020	1	02/01/2020	Informe de los eventos de seguridad	Jefe de SI
2	Solicitar un reporte sobre las incidencias de seguridad	03/01/2020	5	08/01/2020	Conocimiento sobre los eventos de seguridad	Jefe de SI
3	Buscar evidencias acerca de las incidentes	09/01/2020	10	19/01/2020	Conocer más sobre los incidentes	Jefe de SI
4	Realizar una inspección de los incumplimientos	20/01/2020	10	30/01/2020	Conocer que incumplimientos realizan cotidianamente	Jefe de SI
5	Acorde a los incidentes realizar nuevos controles	31/01/2020	5	05/02/2020	Reforzar los incidentes	Jefe de SI
6	Hacer una lista de controles que necesita el área	06/02/2020	10	16/02/2020	Saber sobre los riesgos que puede suceder	Jefe de SI
7	Exponerlo ante el gerente de riesgos	17/02/2020	1	18/02/2020	Aprobación de los controles	Gerente General
8	Realizar una prueba con los eventos existentes	19/02/2020	5	24/02/2020	Conozco que medidas podemos mejorar los eventos existentes	Jefe de SI
9	Ejecución	25/02/2020	5	01/03/2020	Mejorar los riesgos	Jefe de SI

Fuente: Elaboración Propia.

Tabla 18

Plan de actividades con sus respectivas posibilidades

Nro.	Actividad	Justificación
1	Reunión con los Jefe de Continuidad de Negocio	Reunión con el Analista encargado
2	Solicitar un reporte sobre las incidencias de seguridad	Solicitar una lista con tablas específicas de las incidencias
3	Buscar evidencias acerca de las incidentes	Buscar por fechas específicas los incidentes más principales
4	Realizar una inspección de los incumplimientos	Tener una reunión con los jefes de las áreas
5	Acorde a los incidentes realizar nuevos controles	Realizar nuevas políticas
6	Hacer una lista de controles que necesita el área	Lista de las políticas que requieren las áreas
7	Exponerlo ante el gerente de riesgos	Sustentarlo ante el comité de riesgo
8	Realizar una prueba con los eventos existentes	Realizo un cruce de información ante los eventos de riesgos
9	Ejecución	Demostración a todos los colaboradores

Fuente: Elaboración Propia.

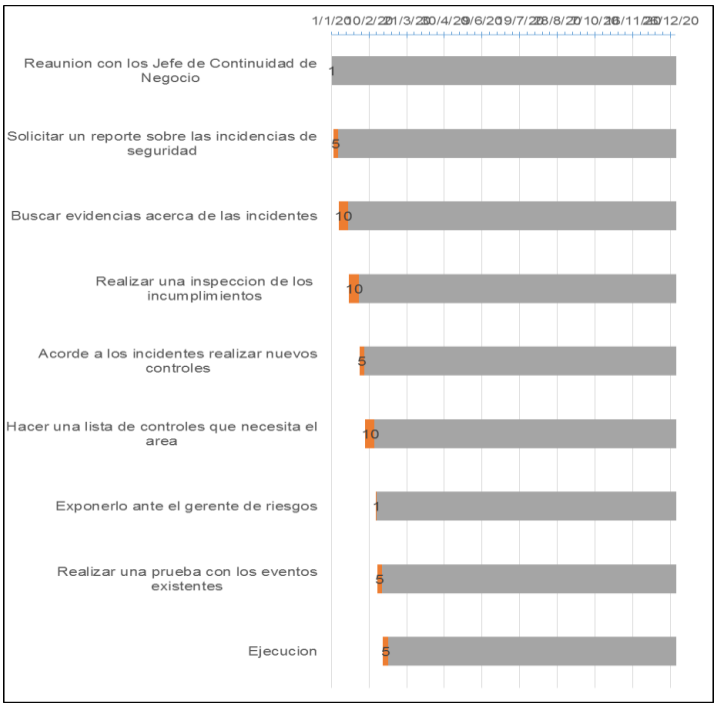


Figura 14. Plan de actividades para los nuevos controles. *Fuente:* Elaboración Propia.

En la figura 14 nos presenta los días de inicio que va realizar cada actividad hasta el último día de la ejecución.

Indicadores:

Para mostrar el segundo objetivo, hemos puntualizado un adecuado indicador que nos muestre el interés propuesto:

Indicador 1:	**Indicador 2:**
$Controles = \frac{N° \ de \ controles}{Total \ de \ eventos \ de \ riesgos} * 100$	$Incumplimientos = \frac{N° \ de \ incumplimientos}{Total \ de \ controles} * 100$

Cuadro 2. Indicadores para los nuevos controles de accesos en los sistemas de la financiera, 2019. *Fuente:* Elaboración Propia.

Los dos indicadores mostrados en el cuadro xx, el primer indicador nos presenta el número de controles que hemos creados y el total de eventos de riesgos, por cien.

Hemos formulado con los eventos de riesgos, ya que queremos comprobar que los eventos que surgen en el área de seguridad de información puede ser solucionado con los controles que hemos propuestos.

También, en el segundo indicador, observamos el número de incumplimientos que puede causar los colaboradores, el total de controles propuestos, por cien. Podemos identificar que con los controles propuestos el área de seguridad de información tiene una mejor forma de solucionar los incumplimientos de los colaboradores.

Ingresos y Egresos del Objetivo Nº2:

Tabla 19

Ingresos y egresos de Objetivo-2

Nro. De Actividades	Ingresos	Egresos	Utilidad/Pérdida
1	0.00	15.00	-15.00
2	0.00	15.00	-15.00
3	0.00	0.00	0.00
4	0.00	15.00	-15.00
5	0.00	15.00	-15.00
6	0.00	499.99	-499.99
7	0.00	0.00	0.00
8	0.00	0.00	0.00
9	0.00	0.00	0.00
Total	0.00	S/559.99	S/559.99

Fuente: Elaboración Propia

En la tabla 19 podemos ver los ingresos y egresos que han tenido todas las actividades, pero según el cuadro la financiera va tener un egreso de S/559.99 soles, en los siguientes cuadros se muestra los egresos que le corresponde a cada actividad:

Tabla 20

Egresos de las actividades 1, 2, 4 y 5

Egresos				
Código	**Descripción**	**Unidad**	**Cantidad**	**Total**
1	Hoja Bond	1	15	15
			Total	S/15.00

Fuente: Elaboración Propia.

En la tabla 20 presenta los egresos de las actividades nº 1- Reunión con los Jefe de Continuidad de Negocio nº2- Solicitar un reporte sobre las incidencias de seguridad, nº4- Realizar una inspección de los incumplimientos y nº5- Acorde a los incidentes realizar nuevos controles, para ser el respectivo actividad usamos de papel hoja bond, para los informes que tenemos que presentar en el momento que se realiza una reunión, para la inspección que se va realizar y para la realización de los controles, lo vamos a presentar en físico cuando lo vamos a exponer ante el gerente de riesgos.

Tabla 21

Egresos de la actividad 6

Egresos				
Código	**Descripción**	**Unidad**	**Cantidad**	**Total**
1	Excel	1	499.99	499.99
			Total	S/499.99

Fuente: Elaboración Propia.

En la tabla 21, evidencia el egreso de la actividad nº6 – Hacer una lista de controles que necesita el área, para poder realizar esta actividad vamos a necesitar el programa Excel, si el responsable no tiene el programa en su pc.

Solución

Propusimos para el segundo objetivo el modelo nuestro objetivo es proponer nuevos controles, segun las actividades que hemos señalado, hemos propuestos nuevos controles, para que ayuden al area de seguridad de información, en la cual estos controles van estar en un excel.

Para desarollar estos controles, nos hemos basado a la ISO 27001, a los controles de accesos, se ha observado que los controles se orientan a usuarios, fundamentado a estos controles hemos propuestos controles apoyado a los activos de información y los usuarios externos. De manera que propuestos estos controles lo contrarestamos con los incidencias cotidianas.

N°	Control
1	Los colaboradores usen con responsabilidades cuando accedan a los activos de información.
2	Los roles y perfiles de los sistemas y aplicaciones este acorde a las funciones de los usuarios.
3	Los proveedores o usuarios externos usen con responsabilidades cuando accedan a los activos de la información.
4	Los colaboradores solo deben manipular los activos de informacion que han sido autorizados por el area de seguridad de información.
5	Las autorizaciones o conformidades deben ser una proceso formal para la habilitacion de acceso en el sistema.
6	Los proveedores o usuarios externos deben aplicar un proceso formal para revisar o usar los documentos secretos, confidenciales y internos.

Figura 15. Lista de controles propuestos. *Fuente:* Elaboracion propia.

Los que hemos propuestos sera una ayuda para poder tener un control en el momento que sucede un incidente que a riesgue nuestro activos de información, en el momento que acceden al sistema. También en cuando suceda un incumplimiento de los colaboradores cuando manejen accedan al sistema y manejen los activos.

Sin embargo, para llevar a cabo la propuesta, desarrollamos un modelo para realizar el inventario de los controles, donde podemos observar el incidente ocurrido, en qué agencia ocurrió el incidente o incumplimiento, la fecha, el estado y el nombre del control que vamos a tomar para llevar a cabo la inspección, iniciando así un seguimiento hasta que se haya solucionado.

Objetivo 3: Elaborar un modelo que ayude optimizar la herramienta que usa el área de seguridad para realizar los monitoreos.

En la tabla 22, se precisa las actividades que se va realizar para poder definir los perfiles en los sistemas, con los siguientes campos, Nro. de actividad, el nombre de la actividad, fecha de inicio y fin, el beneficio que nos va otorgar cada actividad y la persona responsable de cada actividad. También nos muestra en la tabla 23, las actividades con sus respectivas probabilidades que tenemos que seguir, si nos dificultad poder ejecutar las actividades definidas, cerrando así nuestro primer objetivo a realizar.

Actividades:

Tabla 22

Plan de actividades para automatizar los monitoreo de la financiera, 2019.

Nro.	Actividad	Inicio	Días	Fin	Logro parcial	Responsable/s
1	Reunión con jefes de área	01/01/2020	1	02/01/2020	Transmisión de la construcción del modelo	Jefe de SI
2	Aprobación formal del modelo	03/01/2020	5	08/01/2020	Mejorar el proceso actual	Jefe de SI
3	Levantar los sistemas existentes	09/01/2020	20	29/01/2020	Información de los sistemas actuales	Jefe de SI
4	Inventario de sistemas	30/01/2020	10	09/02/2020	Conocimiento de los sistemas existentes	Jefe de SI
5	Armado del modelo	10/02/2020	5	15/02/2020	Identificar los sistemas que van a tener acceso	Jefe de SI
6	Prueba piloto en el área de riesgos	16/02/2020	5	21/02/2020	Verificar de la efectividad del modelo	Jefe de SI
7	Corrección del modelo	22/02/2020	5	27/02/2020	Perfeccionar el modelo	Jefe de SI
8	Permiso de Gerencia General	28/02/2020	2	01/03/2020	Aprobación para la puesta en marcha	Gerente General
9	Ejecución	02/03/2020	5	07/03/2020	Mejorar del proceso	Jefe de SI

Fuente: Elaboración Propia.

Tabla 23

Plan de actividades con sus respectivas posibilidades

Nro.	Actividad	Justificación
1	Reunión con jefes de área	Reunión con los Analista
2	Aprobación formal del modelo	Verificación para la aprobación
3	Levantar los sistemas existentes	Reporte de los sistemas que tienen accesos los colaboradores
4	Inventario de sistemas	Lista de los sistemas de acorde al reporte
5	Armado del modelo	Creación de la estructura
6	Prueba piloto en el área de riesgos	Demo al área de riesgos
7	Corrección del modelo	Sugerencias del modelo
8	Permiso de Gerencia General	Permiso del gerente del área de riesgos
9	Ejecución	Demostración a todos los colaboradores

Fuente: Elaboración Propia.

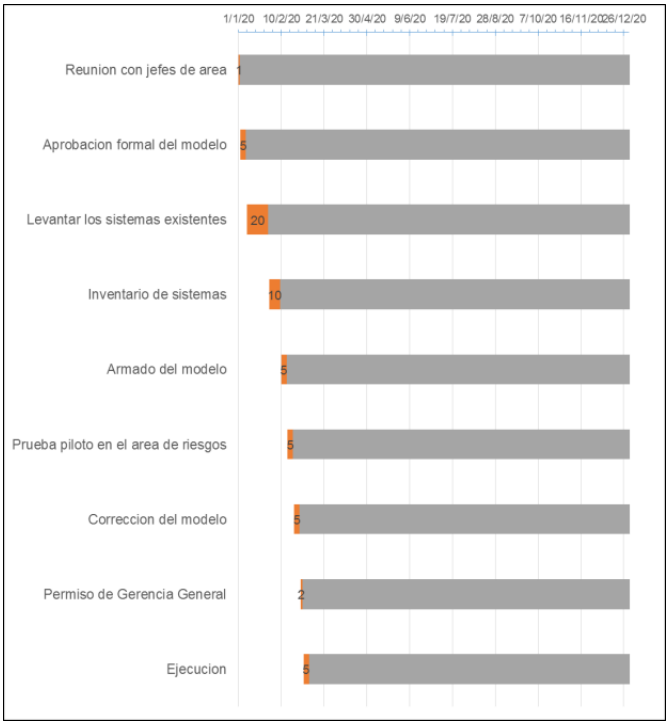


Figura 16. Plan de actividades para automatizar los monitoreo de la financiera, 2019.

Fuente: Elaboración Propia.

En esta figura 16 nos presenta los días de inicio que va realizar cada actividad hasta el último día de la ejecución.

Indicadores:

Para mostrar el tercer objetivo, hemos puntualizado un adecuado indicador que nos muestre el interés propuesto.

Indicador 1:	**Indicador 2:**
$\text{Área} = \frac{Nº\ de\ monitores\ realziados}{total\ de\ monitoreos\ que\ existen\ en\ el\ area} * 100$	$Monitoreos = \frac{N° de\ monitoreos\ ejecutados}{Total\ de\ monitoreos\ programados} * 100$

Cuadro 3. Indicadores para los nuevos controles de accesos en los sistemas de la financiera, 2019. *Fuente:* Elaboración Propia.

Los dos indicadores mostrados en el cuadro xx, el primer indicador nos presenta el número de monitoreos, que existe en el área, con el total de monitores realizados en la financiera por cien. Hemos formulado el número de monitoreos, ya que con el número podemos ver cuantos monitoreos se realizan en la financiera, y el total de monitoreos se contrastaran con los monitoreos que ha realizado el área de seguridad de información.

También, en el segundo indicador, observamos el número de monitoreos programados, con el total de monitoreos ejecutados, por cien. Podemos identificar el número de monitoreos programados, estos monitoreos están en cronograma donde el encargado de realizar el monitoreo sabe cuándo se realiza, ya que saben cuándo el área de TI, le va mandar los reportes para el monitoreo, esto lo vamos a contrarrestar con el total de monitoreos ejecutados que ya haya realizado el área de seguridad de información.

Ingresos y Egresos del Objetivo Nº3:

Tabla 24

Ingresos y egresos de Objetivo-3

Nro. De Actividades	Ingresos	Egresos	Utilidad/Pérdida
1	0.00	15.00	-15.00
2	0.00	15.00	-15.00
3	0.00	15.00	-15.00
4	0.00	499.99	-499.99
5	0.00	2267.00	-2267.00
6	0.00	0.00	0.00
7	0.00	1000.00	-1000.00

8	0.00	0.00	0.00
9	0.00	0.00	0.00
Total	0.00	S/3,811.99	S/3,811.99

Fuente: Elaboración Propia.

En la tabla 24 podemos ver los ingresos y egresos que han tenido todas las actividades, pero según el cuadro la financiera va tener un egreso de S/3,811.99 soles, en los siguientes cuadros se muestra los egresos que le corresponde a cada actividad:

Tabla 25

Egresos de las actividades 1, 2, 3

Egresos				
Código	**Descripción**	**Unidad**	**Cantidad**	**Total**
1	Hoja Bond	1	15	15
			Total	S/15.00

Fuente: Elaboración Propia

En la tabla 25 presenta los egresos de las actividades nº 1 Reunión con jefes de área nº2- Aprobación formal del modelo y nº3- Levantar los sistemas existentes, para ser el respectivo actividad usamos de papel hoja bond, para los informes que tenemos que presentar en el momento que se realiza una reunión, para la inspección que se va realizar y para el levantamiento de sistemas existentes, lo vamos a presentar en físico solicitemos el permiso del gerente general.

Tabla 26

Egresos de la actividad 4

Egresos				
Código	**Descripción**	**Unidad**	**Cantidad**	**Total**
1	Excel	1	499.99	499.99
			Total	S/499.99

Fuente: Elaboración Propia.

En la tabla 26, evidencia el egreso de la actividad nº4 – Inventario de sistemas, para poder realizar esta actividad vamos a necesitar el programa Excel, si el responsable no tiene el programa en su pc.

Tabla 27

Egresos de la actividad 5

Egresos				
Código	**Descripción**	**Unidad**	**Cantidad**	**Total**
1	Compra de licencia de visual studio 2019	1	2,267.00	2,267.00
			Total	S/2,267.00

Fuente: Elaboración Propia.

En la tabla 27, indica que la actividad nº5- armado del modelo, teniendo que comprar la licencia de visual studio 2019, para realizar el prototipo en esa plataforma.

Tabla 28

Egresos de la actividad 7

Egresos				
Código	**Descripción**	**Unidad**	**Cantidad**	**Total**
1	Profesional de apoyo	1	1,000.00	1,000.00
			Total	S/1,000.00

Fuente: Elaboración Propia.

En la tabla 28, nos indica que la actividad nº7- corrección del modelo, va tener un gasto de S/1,000.00 soles, ya que el personal de apoyo su salario va costar este monto.

Solución

Para solucion del tercer objetivo, propusimos el modelo para outomatizar los monitoreos en la financiera y el inventario donde podemos ver la información de los sistemas donde se realizan los monitoreos, esta actividad se realizo basado a una plantilla en excel, donde se ha propuesto automatizar, considerando hacerlo en la plataforma de visual studio, podemos encontrar el prototipo en el Anexo 2: Evidencias de la propuesta, donde podremos ver el modelo planteado, siendo el primer prototipo esta el login, donde el jefe de seguridad de información o el analista podra acceder a traves de su usuario y contraseña.

Segunda prototipo , esta el menu, donde el usuario tendra la opcion de entrar a monitoreos, y tendra la opcion de salir de la plataforma.

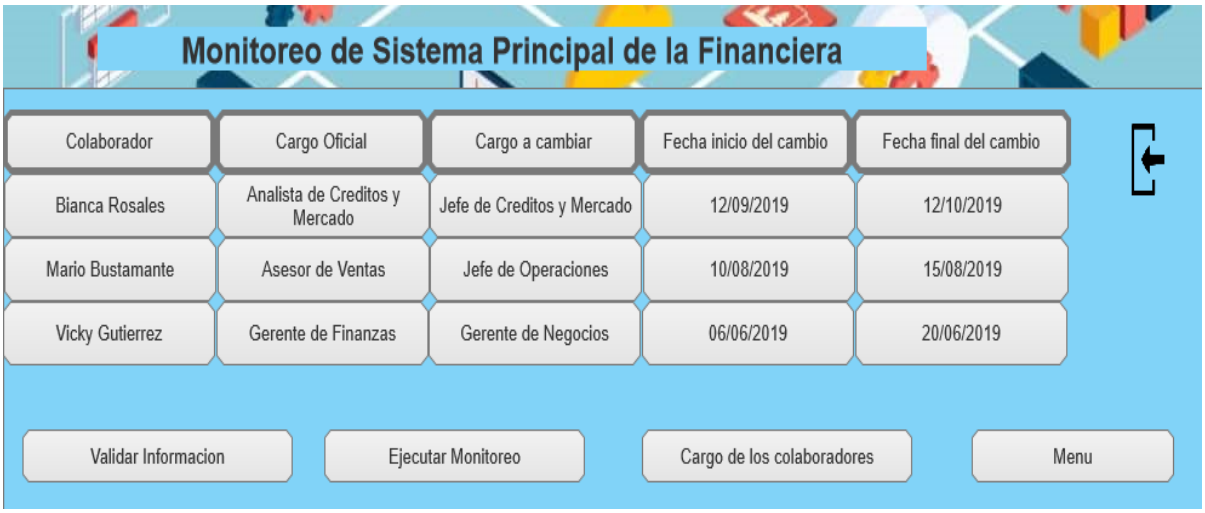


Figura 17. Prototipo de Monitoreo.*Fuente:* Elaboracion Propia.

Tercer prototipo, entrando a la opcion de monitoreos, exportamos el reporte que nos manda el area de TI, ingresado los datos, observamos los cargos que tienen los colaboradores, segun los campos, deben estar en el reporte el cargo oficial, el cargo a cambiar (el cargo temporal o indeterminado que le asigna su area o RR.HH), la fecha de cambio y la fecha final de cambio, se validar la información, si los datos estan correctamente llenado en los campos segun el reporte enviado de TI. Despues ejecuto el monitoreo, donde nos puede salir un aviso, donde haya salido una observacion.

También encontramos el boton de cargo de colaboradores, es una plantilla donde podemos buscar los colaboradores, podemos ver si los colaboradores que ya finalizaron su cambio, estan con su cargo de origen, y tiene la opcion de volver al menu.

Cuarto prototipo, como ya hemos ejecutado el monitoreo, vemos que tenemos una observacion, damos click a verificar obserrvacion, donde podremos ver cual es la observacion.

Quinta prototipo, vemos una observación del colaborador Vicky Gutierrez, podemos ver que su cargo temporal o a cambiar ya finalizo, podemos definir esto, ya que el area de seguridad de información y el area TI, debe tener un acuerdo de cuanto tiempo va demorar el area de TI, para cambiar a los colaboradores a su cargo de origen, entonces enviamos la observacion a TI, tambien tiene la opcion de volver a la plantilla anterior.

Sexta prototipo, ya haciendo click a la observacion a TI, nos sale la observacion que vamos a enviar a TI, para la correccion, hay una espacion en blanco, donde podremos poner nuestros comentarios, para que el area de TI, pueda despues sustentar el motivo de porque el colaborador no fue cambiado a tiempo, damos la opcion a enviar a TI.

Septima prototipo, el area de TI, recibio y observo cual es el comentario que envio seguridad de información a TI. De manera que el area de TI, sustenta el motivo y envia a segurida de información su motivo.

Obtavo prototipo, el analista o jefe de seguridad de información podra ver el sustento y definira si su sustento sera tomada como observacion, para corroborar si Vicky Gutierrez tien sus cargo de origen, podremos volver al modelo del monitoreo y dar la opcion de cargo de colaboradores y ver si el colaborador tiene su cargo de origen.

También se realizó el inventario de sistemas existentes de la financiera, siendo una propuesta para tener un mayor control de los sistemas que tiene, considerado los siguientes campos: n° de sistemas, nombre del sistema, descripción, tiempo de recuperación que puede tardar el sistemas en momento que se realice una falla, en la opción de backup; esta el campo de periodo, podemos ver si la copia de seguridad de se realiza diario, mensual o semanal; también el campo de días que se va almacenar, se puede definir de acuerdo al sistema que día se necesita que se tenga la copia de la información y almacenar, acá se ve dónde va estar la data. Podemos ver el cargo que tienen accesos a los sistemas.

4.4 Discusión

En la investigación titulada “Diseño de un modelos de control de accesos a los sistemas de información basado en la ISO 27001 en una financiera, Lima 2019.”, el objetivo es proponer controles y herramientas que disminuya el incumplimiento de privacidad de la información en la mejora del proceso de gestión de control de accesos a los sistemas y aplicaciones en las Financieras de Lima, se implanto con la compilación de las entrevistas y cuestionado realizado en la áreas correspondiente de la financiera, con los treintas entrevistas y encuestas pudimos hallar problemas que tiene el área de seguridad de información en la financiera, obteniendo objetivos, y propuestas para dar una solución al problema que sucede en la financiera. Según los diagnósticos que hemos obtenido de las entrevistas y cuestionarios, en las categorías políticas de acceso, se identificó la categoría emergente activos de información, como en la categoría en el ítem 3, se puede ver que el 33% de los colaboradores cumplen con los controles de acceso de seguridad entre a veces, normalmente y casi siempre manejan la información de los clientes, mientras el 3% siempre cumplen con los controles de acceso de seguridad, identificando que las acciones de los colaboradores también involucran a los activos información, ya que estos son los que van a manejar los colaboradores, acorde con De Freitas (2008) detalla que la organización debe entender que las amenazas que pueden ser atacadas son los activos de información, siendo un gran reto para la entidad en tener siempre estrategias para alegar los ataques que vulneren su estabilidad, proponiendo una gran acción a tomar cuando ejecutan controles para evitar estas incidentes. Sin embargo se propuso la creación de controles para llevar a cabo estas incidencias y también un modelo para definir de forma organizada los perfiles que tienen los colaboradores, se tomó las medidas de llevar desarrollar los controles ya que Carrillo (2011) puntualiza que la teoría de control un método de poder inspeccionar un procedimiento del sistema, para siga manejando con indicadores específicos, siendo este examen un grupo de herramientas que trabaja de manera vertical para tener un resultado o una contestación. Siendo los controles creados para tener un control del riesgo que tiene la financiera ante una amenaza que dificulte la función de la entidad, llevando este control un proceso de ejecución hasta llevar a la solución o prevención de los incidentes. De manera que la categoría políticas de acceso en el ítem 5, el 33% de los colaboradores indicaron que los accesos que se le otorgan a los colaboradores casi siempre tengan restricciones de

seguridad, mientras el 13% siempre tienen acceso con sus respectivas restricciones de seguridad, dando como propuesta el modelo de automatizar las herramientas que tiene la financiera para realizar sus monitoreos, esto es acorde a que con este modelo nos permite ver qué perfil tiene acceso a los sistemas respectivos, que opciones tiene en el sistema, a que carpeta compartida tiene acceso, entre otros, siendo Uscatescu (1973) detalla que la teoría de la información define que es una conexión entre la información o datos semejantes, viendo que las descripciones de la información sean semejantes y no información alteradas que reflejen errores, teniendo medio para verificar que todo lo expuesto en la información es auténtico y claro. También se definió en la categoría sistemas y aplicaciones, se identificó la categoría emergente, perfiles y roles, esta categoría se nombró, ya que en el ítem 14 se observa el 50% de colaboradores opina que todos los sistemas que usa el colaborador tienen a veces definidos los roles y perfiles según los cargos que tiene, mientras que el 10% de los sistemas siempre tiene definidos los roles y perfiles, viendo que los perfiles y roles, es el primer escala de crear un cargo en el sistema, de manera que Zapata y Ceballos (2010) especifica que los perfiles y roles se desarrolla cuando se tiene establecido el rol del cargo, siendo esto importante para tener una conexión con el perfil que tiene en el sistema, identificando los roles que tendría el perfil, siendo los roles las opciones que tendría el colaborador en el momento que maneje el sistema. Para el ítem 14, propusimos el modelo donde esta definidos los perfiles que tiene el sistema de la financiera, acorde a Ruiz (1994) precisa que la teoría del mosaico pronuncia que la información privada y pública, es función que tiene la persona y la utilidad que le da el otro usuario que gestiona la información. De manera que la información sumamente importante debe estar protegida por el hurto y robo de información, según este fundamento vemos que los perfiles que se le otorgan a los colaboradores es fundamental en tener un control de estos, ya que es la puerta que tiene el colaborador cuando accede a los activos de información. Finalmente con los modelos propuestos se quiere dar a conocer a las áreas de seguridad de información, de las diferentes entidades financieras, cajas, etc. que los modelos manuales que utilizan pueden ser automatizados para poder tener a tiempo sus actividades y poder tener un mayor control de los accesos que tienen los colaboradores cuando manejan sus activos de información, siendo esto un riesgos para las entidades financieras.

CAPÍTULO V

CONCLUSIONES Y SUGERENCIAS

5.1 Conclusiones

Primero: Se propone establecer controles y herramientas para disminuir el incumplimiento de privacidad de la información en la mejora del proceso de la gestión de control de accesos a los sistemas y aplicaciones en las financieras, de esta manera se podrá solucionar los problemas relacionados a los riesgos de la financiera, otorgándole al área de seguridad de información confiabilidad cuando use dichos controles y herramientas.

Segundo: También, se propone desarrollar un modelo para definir los perfiles, siendo estos perfiles que van a relacionar con los sistemas y aplicaciones de la financiera, dando a los colaboradores accesos según su cargo, diagnosticando al área de seguridad de información una posición más frecuente ante los cargos que tienen accesos a los sistemas, como por ejemplo accesos a carpeta compartida, a usb, entre otros.

Tercero: Se propone la creación de nuevos controles de accesos de seguridad de información, siendo los controles como un valor para disminuir las incidencias que pueda ocurrir en cualquier momento la financiera, ya que las incidencias pueden ocasionar vulnerabilidades y amenazas, siendo estos controles un medio de control cuando ocurra una incidencia, llevándolo a controlar a través de una plantilla donde se ejecutara los controles con las incidencias.

Cuarto: Se propone hacer un modelo que ayude al área de seguridad de información en el momento que realice el monitoreo del sistema principal de la financiera, dando al área de seguridad de información una mejora en el uso en el momento que monitorea, siendo automatizado para modernizar las estrategias que tiene el área para controlar sus accesos en los sistemas y aplicaciones, siendo una gran influencia en las demás áreas y la entidad financiera.

5.2 Sugerencias

Primero: Sugerimos que estos controles y herramientas se pueda implementar en el área de seguridad de información, con la ayuda de poner en practica la ley de protección de datos personales, declaraciones que puedan a influenciar en minimizar los riesgos y las demás normas Iso que influyan al área de seguridad de información, en mejorar sus forma de trabajo con los objetivos de la organización..

Segundo: También sugerimos que los modelos para establecer bien definidos los perfiles en el sistema y aplicaciones, se pueda efectuar en las financieras y en el área de seguridad de información, ya que dicho modelos pueda controlar los accesos que tienen dicho perfil según el cargo que tiene el colaborador de la financiera, dando al área confiabilidad en el momento que realice el monitoreo de perfiles.

Tercero: Sugerimos inspeccionar los eventos o incidentes bajo la lista de controles propuestos para la financiera, bajo la norma I SO 27001, ejecutando esta medida bajo capacitaciones a los colaboradores sobre activos de información, plan de acción, vulnerabilidades, riesgos, entre otros, para llevar estos controles como medida de control cuando suceda una incidencia en la financiera, cooperativa de ahorro o banco.

Cuarta: Sugerimos automatizar las herramientas de los monitoreos que maneja el área de seguridad de información de la financiera bajo el modelo propuesto, ya que dicho monitoreo podrá dar al área un control cuando los colaboradores excedan de dichos accesos que no le corresponde según su cargo, llevando con la plantilla de inventario de activos de sistemas una medida de controlar que sistemas son prioritarios para la financiera.

CAPÍTULO VI

REFERENCIAS

Acosta, X. (2015). *Desarrollo de un modelos de seguridad para la prevención de pérdida de datos dlp, en empresas pymes.* Quito.

Aguirre, D. (2014). *Diseño de un Sistema de Gestión de Seguridad de Información para servicios Postales del Perú S.A.* Lima: Universidad Pontifice Católica del Perú.

Alcala, H. (1998). *El Derecho a la privacidad y la intimidad en el ordenamiento juridico chileno.* Chile: Universidad de Talca.

Alvarado, F. (2016). La gestión de la Seguridad de la Información en el régimen. Lima: Revista Foro Jurídico. (Vol. 15, págs. 26-41).

Aparicio, J. (2017). *Conceptos y legislación de transparencia sindical y protección de datos personales de los trabajadores en México.* Mexico: Universidad Nacional Autònoma de Mexico.

Arabany Ramirez, L. (2002). *Teoría de Sistemas.* Colombia: Universidad Nacional de Colombia.

Bertalanffy, L. (1976). *Teoría General de los Sistemas.* Mexico: Fondo de Cultura Economica.

Betancur, P. (2009). *Aplicación del modelo de sistemas de producción y medios de vida a un caso rural del Departamento de Risaralda. Manizales, Caldas,* Colombia: Revista Luna Azul. (Vol. 28, págs. 68-85).

Bustamante, J. (2017). *Lineamientos basicos de una investigación estadistica.* Dirección de Regulación, Planeación,Estandarización y Normalización (DIRPEN) .

Cabrera, G., Londoño, J. & Bello, L. (2008). *Validación de un instrumento para medir calidad percibida por usuarios de hospitales de colombia.* Colombia: Universidad de Antioquia. Medellín.

Calderon, J. (2009). *El derecho de los contribuyentes al secreto tributario.* España: Editorial Netbiblo.

Canales, M. (2006). *Metodología de investigación social.* Chile: LOM ediciones.

Carazo, O. (2013). *Elaboración de un Plan de Seguridad de la Información.* España: Universidad Oberta de Catalunya.

Cardozo, M. (2013). *Políticas públicas: los debates de su análisis y evaluación.* Mexico: Andamios. (Vol. 10, págs. 39-59).

Carrasco, S. (2015). *Análisis de la aplicación de la tecnología móvil en las empresas.* Obtenido de Universidad Politecnica de Valencia, España.

Carrillo, P. (2011). *Sistemas Automáticos de Control. En Fundamentos Basico de Analisis y Modelado.* Venezuela: Fondo Editorial Universidad Nacional Experimental.

Carrión, I., Fernández, J., & Toval, A. (2011). *Gestión del control de acceso en historiales clínicos electrónicos: revisión sistemática de la literatura.* Barcelona: Gac Sanit. (Vol. 26, págs. 463-468).

Casado, M. (2016). *Control de acceso a red de nueva generación.* Lima: Red Seguridad.

Cauas, D. (2015). *Definición de las variables, enfoque y tipo.* Francia: Calameo. (Vol. 1, págs. 1-11).

Cedeño, W., & Muñoz, S. (2000). *Control de gestión y Gestión tecnológica.* Brasil: Revista Redalyc. (Vol. 4, págs. 85-97).

Cerpa, E. (2009). *Introduccion a la Teoria de Contro.* Venezuela: Universidad Santa Maria.

Credinka, F. (s.f.). *Financiera Credinka.* Lima: Financiera Credinka.

Cuenca, J. (1999). *"Física, teoría de la información y economía: tres lugares comunes para la entropía".* España: Universidad Autonoma de Madrid.

Dailey, R. (1990). *Comportamiento Organizacional.* Edinburgh : Escuela de Negocios de Edimburgo - Heriot-Watt University.

Dextre, J., & Pozo, R. (2012). Administracion. En *Control de gestión o gestión de control?* . Lima, Peru: Revista Redalyc.(Vol. 7, págs. 69-80)

Diaz, S. (2014). *Los métodos mixtos de investigación: presupuestos generales y aportes a la evaluación educativa.* Portugal: Revista Portuguesa de Pedagogia. (Vol. 48, págs. 7-23).

Dirección Nacional Seguridad, p. (2019). *Metodologia para la gestión de la seguridad informatica.* Cuba: Oficina de Seguridad para las redes informaticas.

Domínguez, L. (2012). *Analisis de Sistema de Información.* Mexico: Red Tercer Milenio.

Dussan, C. (2006). *Políticas de seguridad informática.* Lima: Revista Redalyc. (Vol. 2, págs. 86-92)

Eguiguren, P. (2015). *El derecho a la protección de Datos Personales Algunos temas relevantes de su regulación en el Perú.* Lima, Peru: Revista Universidad Pontifice Católica del Perú.(Vol. 67, págs. 131-140).

Espinoza, H. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.* Lima: Repositorio Universidad Pontifice Católica del Perú.

Gallardo Echenique, E. (2017). *Metodología de la Investigación: manual autoformativo interactivo.* Huancayo, Peru: Repositorio Continental.

Gallarzo, M., Espinoza, J., & Hernandez, J. (2011). *Desarrollo Organizacional.* Mexico: Pearson Educacion por Mexico.

Gallego, A., & Ruiz, A. (2010). *La concienciación previa es un complemento imprescindible contra la pérdida de información.* Lima: Red de Seguridad.

García, C., & Fernández, M. (2002). *Teoría de la Información y Codificacion.* España: Universidad de Vigo.

Gerencia, R. (2010). *Control de acceso.* Chile: Revista Gerencia-Noticias, analisis e informacion. (Vol. 1, págs. 1).

Haza, A. (2015). *No se lo Digas a nadie, pero tengo un banco de Datos de Clientes Sensibles, La Gestión de la Protección de Datos de Personales en el Sistemas Financiero para la Prevención de Lavado de Activos.* Lima, Peru: Revista de Actualidad Mercanti, Universidad Pontifice Católica del Perú. (Vol. 4, págs. 74-93).

Henriquez, C. (2010). *Sistema de control de acceso basado en Java Cards y Hardware libre.* Mexico: Revista Redalyc. (Vol. 8, págs. 63-68).

Hernández Sampieri, R. (2014). *Metodología de la Investigación.* Mexico: Mc Graw Hill Education / Interamericana Editores S.A.

Herrera, P. (2016). *El derecho a la vida privada y las redes sociales en Chile.* Chile: Revista Chilena de derecho y tecnología. (Vol. 5, págs. 87-112).

Hurtado de Barrea, J. (2010). *Guía para la comprension holistica de la ciencia.* Venezuela: Universidad Nacional Abierta Direccion de Investigacion y Postgrado.

IBM. (2012). *Gestione identidades y el acceso para una continua conformidad y una reducción de riesgos.* EE.UU: IBM Corporation.

Iscara, S. (2014). *Manual de investigación cualitativa.* Lima, Peru: Ministerio de Educación.

Johansen, B. (1982). *Introducción a la Teoría General de Sistemas.* Mexico: LIMUSA Grupo Noriega Editores.

Juarez Varas, M. (2017). *Ingenieria Nacional.* Lima: Colegio de Ingenieros del Peru. (Vol. 23, págs. 4-66).

López, C., & Veiga, M. (2002). *Teoría de la Información y Codificación.* España: Universidad de Vigo.

Lopez, P. (2004). *Población, Muestra y Muestreo.* Bolivia: Punto Cero. (Vol. 1, págs. 69-74).

Maya, E. (2014). *Metodos y tecnicas de investigación.* Mexico: Universidad Nacional Autonoma de Mexico. (Vol. 1, págs. 69-74).

Mendoza, J., & Garza, J. (2009). *La medición en el proceso de investigación cientifica.* Mexico: Revista Universidad Autónoma de Nuevo León, Innovaciones de Negocios. (Vol. 6, págs. 17-32).

Miranda, R. (2012). *Principales acusaciones contra su obra.* España: Revista Infoamerica. (Vol. 7, págs. 145-158).

Moguel, J. (2012). *Aportaciones del desarrollo organizacional a la responsabilidad social de las empresas.* Mexico: Universidad Autónoma de Chiapas. Administracion para el desarrollo.

Monsalve Caballero, V. (2016). *La Protección de Datos de Carácter Personal en los Contratos Electrónicos con Consumidores: Análisis de la Legislación Colombiana y de los Principales Referentes Europeos.* Mexico: Revista Prolegómenos. (Vol. 1, págs. 163-195).

Montesino, R., Baluja, W., & Porven, J. (2013). *Gestión automatizada e integrada de controles de seguridad informática.* Cuba: Revista de Ingenieria Electronica, Automatica y Comunicaciones. (Vol. 34, págs. 40-58).

Montoya, J., & Restrepo, Z. (2012). *Gestión de identidades y control de acceso desde una perspectiva organizacional.* Colombia: Revista Ingenierias USBMed. (Vol. 3, págs. 23-34).

Montufar Guizar, R. (2013). *Desarrollo Organizacional principio y aplicaciones.* Mexico: McGRAW-HILL/INTERAMERICANA EDITORES, S.A.

Mora Perez, A. (2016). *Gestión de Prevención. Control de acceso.* España: Repositorio Universidad Policitenica de Cartagena.

Mora, F. (2002). *Antologia de metodos cualitativos en la investigación social.Revista Región y Sociedad.* (Vol. 14, págs. 236-240).

Morales tejada, S. (2019). *Prototipo de Control de Acceso Peatonal al Campus de la Corporación Universitaria.* Colombia: Corporación Universitaria Lasallista.

Otzen, T., & Manterola, C. (2017). *Tecnicas de muestreo sobre una población a estudio.*Chile: Scielo. (Vol. 35, págs. 227-232).

Perez, M., Hidaldo, A., & Berenguer Perez, E. (2008). *Introducción a los sistemas de control y modelo matemático para sistemas lineales invariantes en el tiempo.* Argentina: Universidad Nacional de San Juan.

Rivas Arellano, M. (2016). *Implementación de un sistema de control de acceso para mejorar la seguridad de información de la empresa SNX S.A.C.* Lima: Repositorio Nacional Mayor de San Marcos.

Roble, F., & Jose, A. (2016). *Definiendo la hipertextualidad. Análisis cuantitativo y cualitativo de la evolución del concepto.*España: Revista Dialnet. (Vol. 14, págs. 1-68).

Rodríguez Rodríguez, J., & Daureo Campillo, M. (2003). *Sistemas de información: Aspectos tecnicos y legales.* Mexico: Universidad de Guadalajara.

Ruiz, C. (1994). *En torno a la protección de los datos personales automatizados.* España: Revista de Estudios Políticos. (Vol. 84, págs. 237-264).

Santana, C., Tavares, G., Miranda, L., Custodio, A., Chaves, C., & Oliveira, P. (2017). *La aplicación del proceso informático de enfermería: revisión integradora.* España: Revista Electronica de Enfermeria. (Vol. 48, págs. 603-619).

Sanz Salguero, F. (2015). *Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado.* Colombia: Revista Ius et Praxis. (Vol. 22, págs. 323-376).

Sarabia, A. (1995). *La Teoría General de Sistemas.* España: Isdefe Ingenieria de Sistemas.

Smith, C., & Corripio, A. (1991). *Control Automatico de Procesos* . Mexico: EDITORIAL LIMUSA.

Tamayo, A. (1999). *Teoría General de Sistemas.* Colombia: Universidad Nacional de Colombia.

TI, R. B. (2019). *Las entidades financieras ante las crecientes amenazas de ciberseguridad.* Lima: Redaccion Byte TI.

Tocancipa, A. (Universidad Nacional de Colombia de 1976). *Teoría de Control.* Colombia: Repositorio institucional Universidad Nacional de Colombia.

Tola Franco, D. (2015). *Implementación de un sistema de Gestión de la Seguridad de la Información para una empresa de consultoría y auditoria, aplicando la norma ISO/IEC 27001.* Ecuador: REPOSITORIO DE ESPOL.

Torres Nafarrate, J. (1996). *Introducción a la teoria de Sistemas.* Mexico: Universidad Iberoamericana, A.c.

Uscatescu Barron, J. (1973). *Teoría de la Información.* España:Revista de estudios politicos. (Vol. 192, págs. 53-74).

Valencia Duque, F., & Orozco Alzate, M. (2015). *Metodología para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 2700.* Colombia: Revista Ibérica de Sistemas y Tecnologias de Información. (Vol. 22, págs. 73-88).

Yumi, J., & Urbano, C. (2014). *Tecnicas para investigar - Recusos Metodologicos para la prepación de proyectos de investigación.* Argentina: Editorial Brujas.

ANEXOS

Anexo 1: Matriz de la investigación

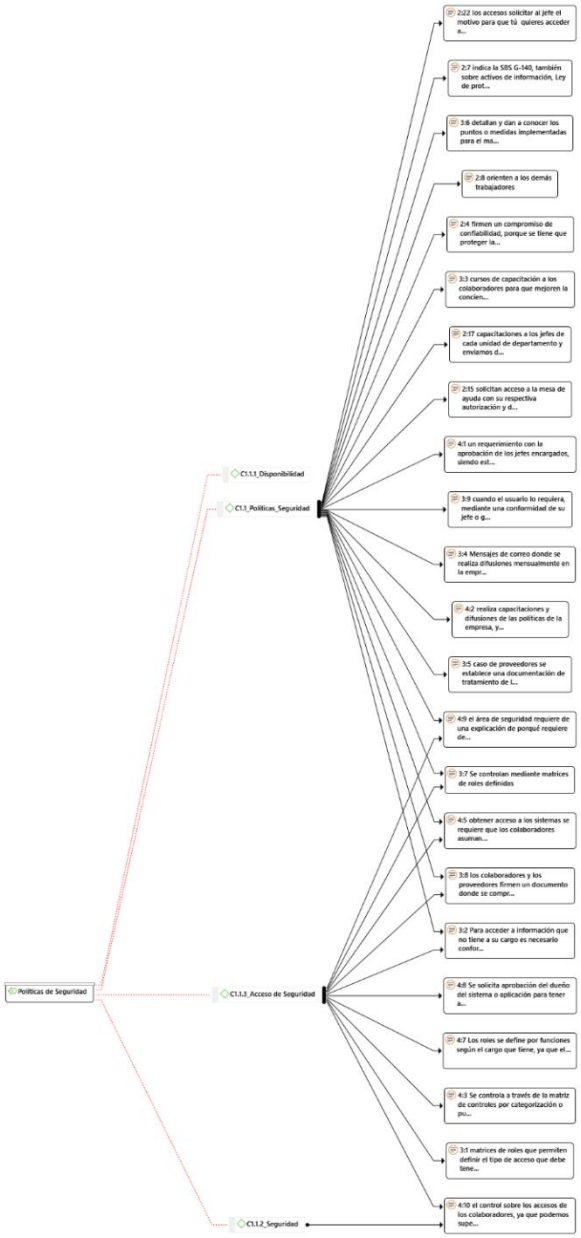
Problema general	Objetivo general	Categoría: Gestión de Control de Acceso			Escala				
		Sub categorías	Indicadores	Ítem	N	A	Nt	Cs	S
¿Cómo mejorar el control de accesos de los sistemas y	Proponer controles y herramientas que disminuya el incumplimiento de privacidad de la	Políticas de Accesos	Disponibilidad	¿Cuándo un trabajador comienza a elaborar y asumir sus funciones se le otorgan sus respectivos usuarios al sistema de la financiera?	1	2	3	4	5
				¿Solicita permisos para ingresar a información secreta, confidencial y interna que no tiene que ver con su cargo?	1	2	3	4	5
¿Aplicaciones en una entidad Financiera, 2019?	Información en la mejora del proceso de gestión de control de accesos a los sistemas y aplicaciones en las Financieras de Lima, 2019.		Seguridad	¿Los colaboradores cumplen con los controles de acceso de seguridad cuando manejan la información de los clientes?	1	2	3	4	5
				¿Considera Ud. Que la financiera cumple con las políticas de seguridad de información para salvaguardar la información?	1	2	3	4	5
			Accesos de Seguridad	¿Considera Ud. que los accesos que se le otorgan a los colaboradores tengan restricciones de seguridad?	1	2	3	4	5
				¿Que la información que usas tienen controles de seguridad en los sistemas y aplicaciones de la empresa?	1	2	3	4	5
				¿Cuándo se le otorga acceso a los jefes y los proveedores crees que se le debe restringir los accesos que no están a su cargo?	1	2	3	4	5
		Control de Acceso	Compromiso con los colaboradores	¿Ha recibido alguna documentación donde se comprometa a usar con responsabilidad la información que maneja y usa en el sistema de la empresa?	1	2	3	4	5
				¿Los proveedores cuando inician un contrato con la financiera firman un contrato de confiabilidad?	1	2	3	4	5
			Medidas de accesos	¿Cuándo se le otorga acceso a los colaboradores se requiere de alguna conformidad del jefe o gerente encargado?	1	2	3	4	5
¿Cómo es el control de accesos de los	Diagnosticar la situación de la gestión de control de accesos			¿Cuándo comparten documentos confidenciales a proveedores o a la SBS, se requiere de conformidad del jefe o gerente?	1	2	3	4	5

sistemas y aplicaciones en una entidad financiera, Lima 2019?	de los sistemas y aplicación en la Financiera de Lima, 2019.		Inducción	¿Ha recibido inducción sobre el manejo de la información cuando accede al sistema de la empresa?	**1**	**2**	**3**	**4**	**5**
Cuáles son las causas de mayor amenaza en los controles de accesos de los sistemas y aplicaciones de una entidad Financiera, 2019?	explicar las causas de mayor importancia que ocasionan vulnerabilidades en la gestión de control de accesos de los sistemas y aplicaciones en una entidad Financiera, 2019			¿Considera ud. Que se debería orientar a los colaboradores acerca de las responsabilidades que tiene el usuario cuando usa información de la empresa?	**1**	**2**	**3**	**4**	**5**
		Sistemas y Aplicaciones	**Uso**	¿Todos los sistemas que usa el colaborador tienen definidos los roles y perfiles según los cargos que tiene?	**1**	**2**	**3**	**4**	**5**
				¿Los sistemas que manejan los colaboradores tienen un usuario clave y contraseña?	**1**	**2**	**3**	**4**	**5**
¿Cómo las estrategias influyen en el control de accesos de los sistemas y aplicaciones en una entidad Financiera, 2019?	Predecir la influencia de las estrategias en la gestión de control de accesos de los sistemas y aplicaciones en una entidad Financiera, 2019.		Acceso	¿Considera ud. Que los controles no automatizados que tienen la empresa son de utilidad para verificar los accesos indebidos?	**1**	**2**	**3**	**4**	**5**
				¿Para obtener accesos a los sistemas y aplicaciones que no están asignados según mi cargo, se requiere de la autorización de mi jefe o gerente?	**1**	**2**	**3**	**4**	**5**
			Monitoreo	¿Se realiza un adecuado monitoreo de los accesos que se le otorgan a los colaboradores de la empresa?	**1**	**2**	**3**	**4**	**5**
				¿Ha observado ciertas irregularidades en el momento que los colaboradores usen la información de los clientes?	**1**	**2**	**3**	**4**	**5**
				¿Recibe la empresa un informe diariamente?	**1**	**2**	**3**	**4**	**5**

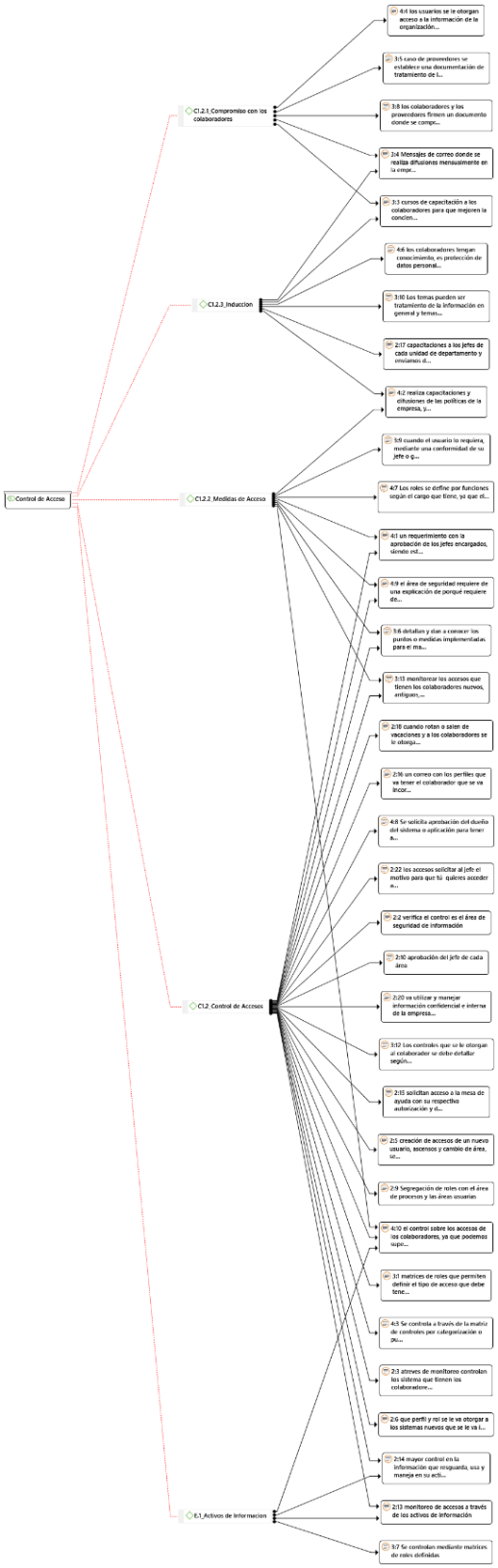
Población, muestra y unidad informante	**Técnicas e instrumentos**	**Procedimiento y análisis de datos**
Población: 60 colaboradores Muestra: 30 colaboradores Unidad informante: División de Riesgos	Técnicas: Encuesta o entrevistas. Instrumentos: Hoja de encuesta o cuestionario.	Procedimiento: elaboración de documentos y controles para la protección de datos personales en la herramientas para la gestión de control de acceso.

Anexo 2: Evidencias de la propuesta

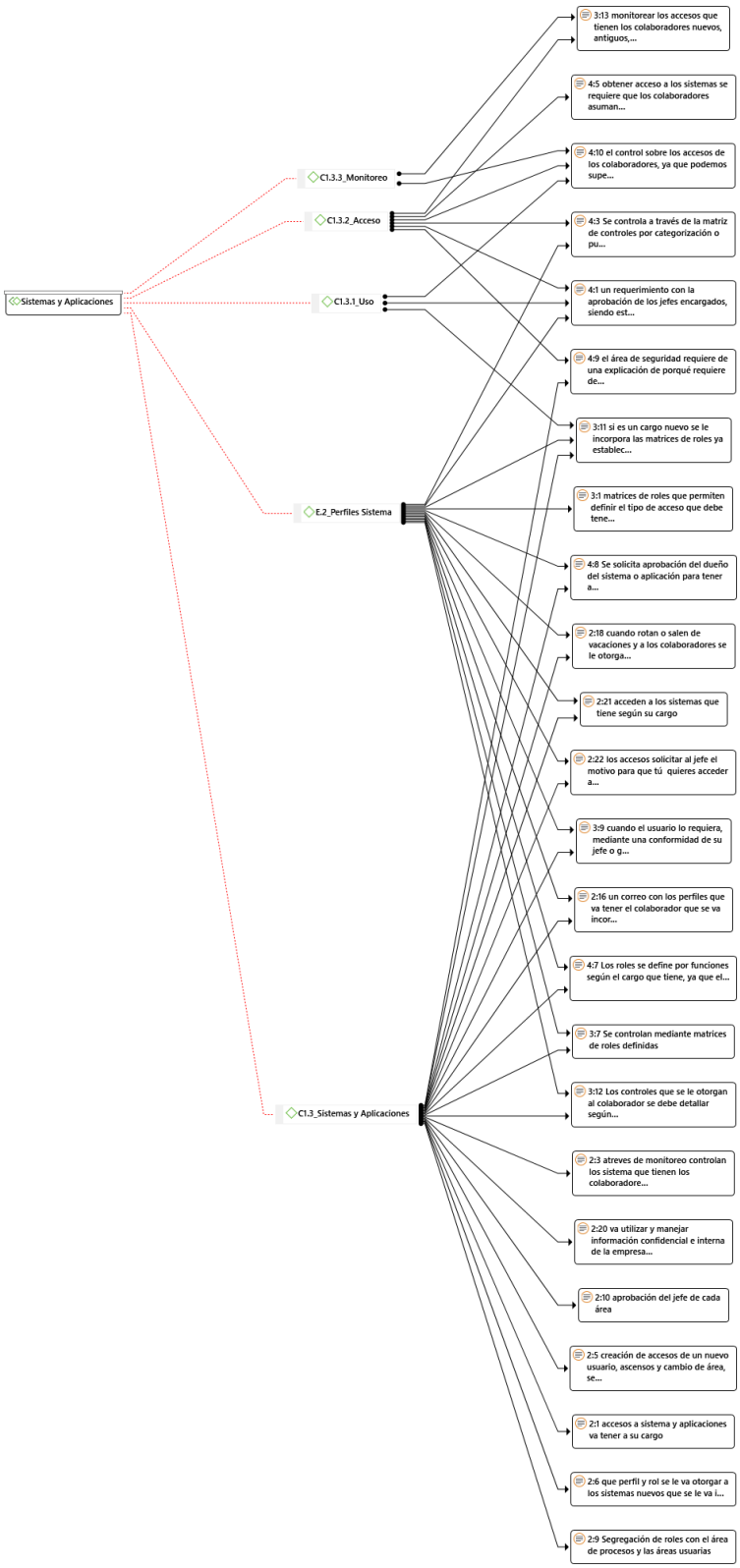
Análisis cualitativo



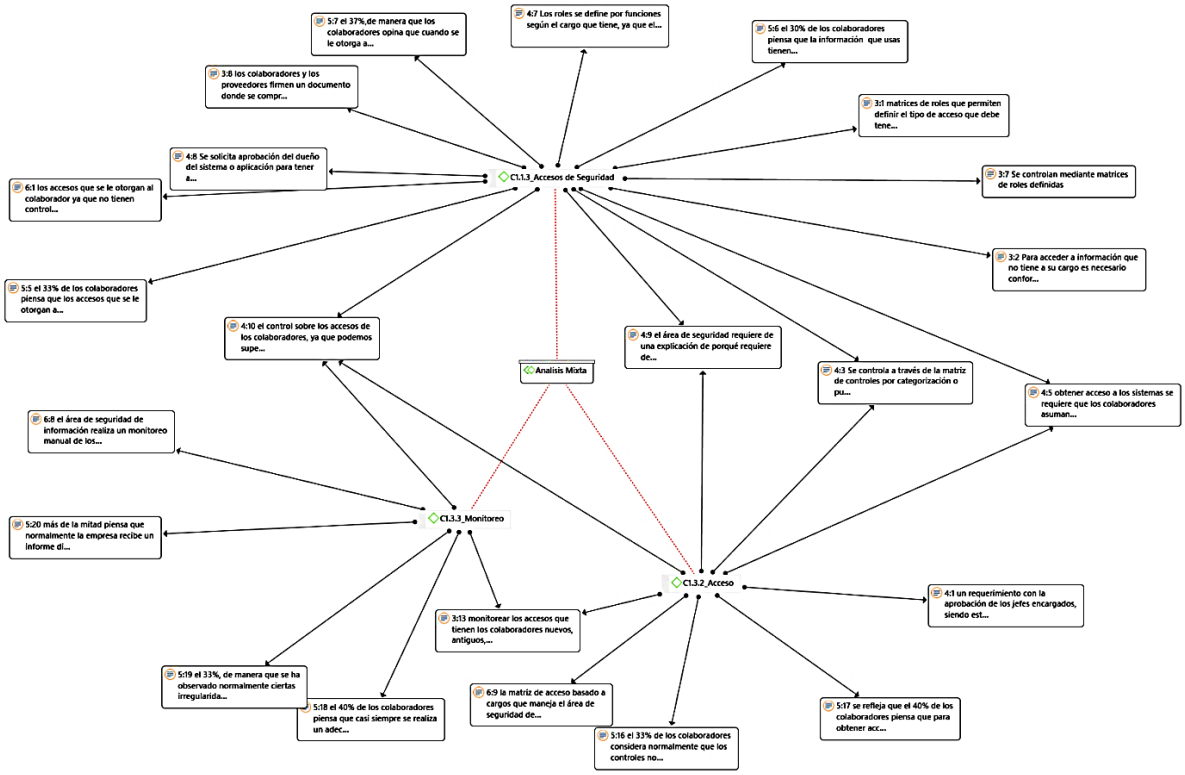
Red informativa de la subcategoría políticas de accesos



Red informativa de la subcategoría control de acceso



Red informativa de la subcategoría sistemas y aplicaciones



Red mixta de la gestión de control de accesos

Prototipo de los objetivos propuestas

Objetivo 1. Modelo de accesos y perfiles

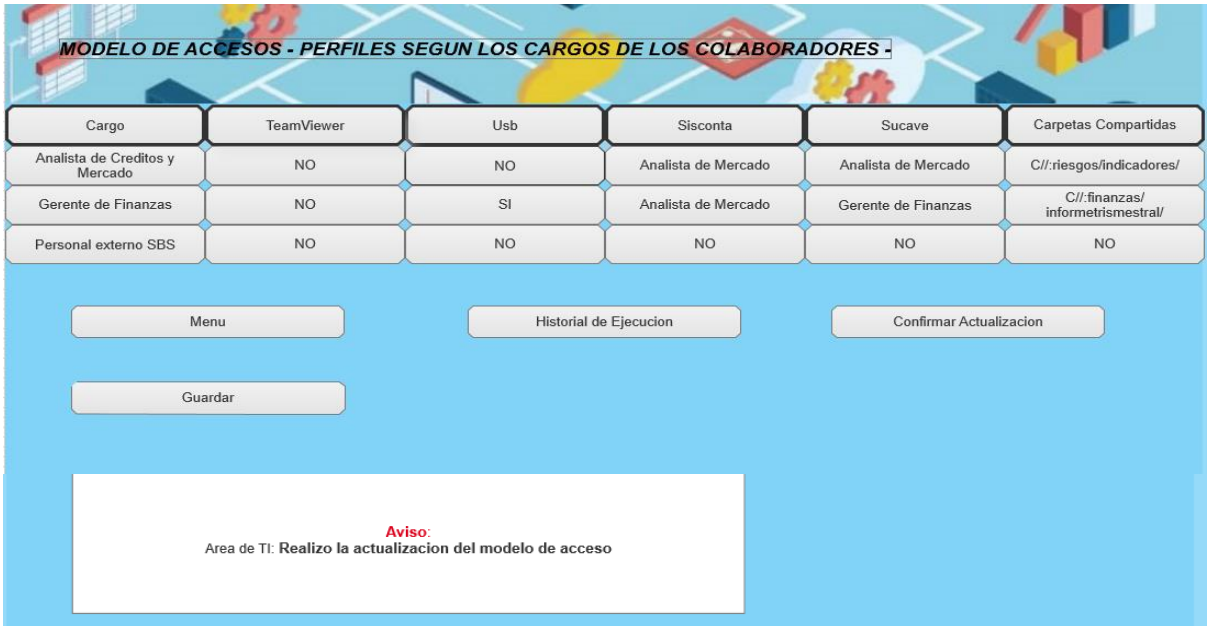
Cargo	TeamViewer	USB	Sisconta	Sucave
Analista de Creditos y Mercado	NO	NO	Analista de Mercado	Analista de Mercado
Gerente de Finanzas	SI	SI	Analista de Mercado	Gerente de Finanzas

Plantilla en Excel modelo de accesos

Login del prototipo

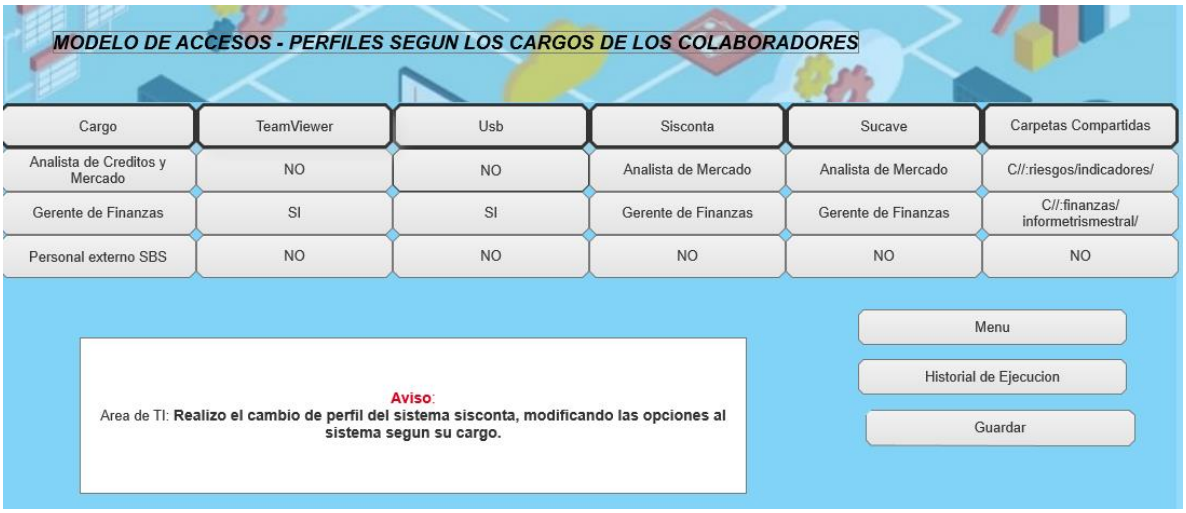
Menú del modelo

Propuesta del modelo de acceso a perfiles



Ejecución de un cambio de perfil

Aviso del cambio realizado al área de TI



Comunicado del área de TI

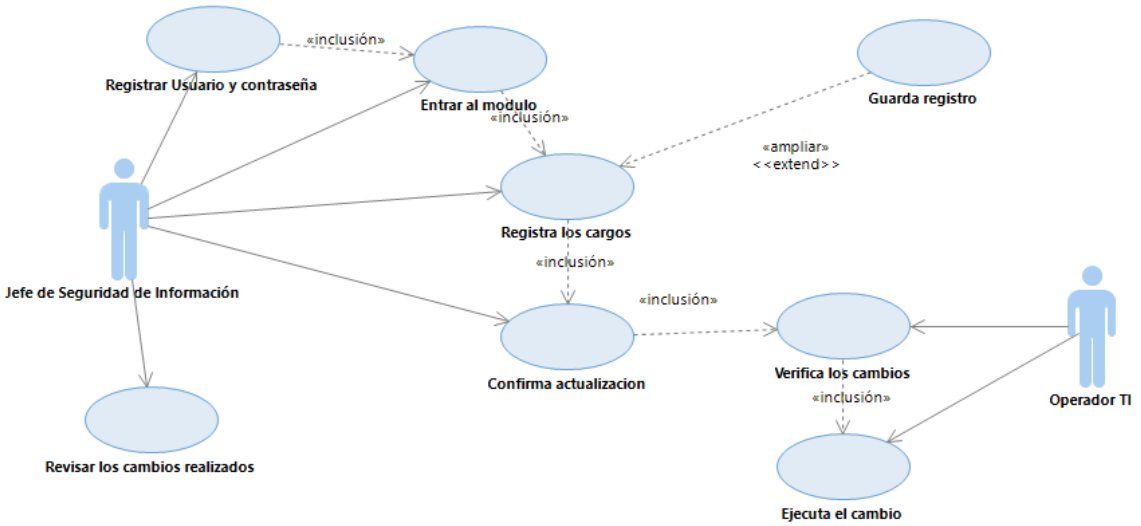


Diagrama de caso de uso del modelo propuesto

					Backup lost
N°	Perfiles	Area	Cargo	Sistemas/Aplicaciones	Areas Primordiales
1	Analista de Mercado	Credito y Mercado	Analista de Creditos y Mercado	Sisconta -Sucave	1
2	Gerente de Finanzas	Finanzas y Contabilidad	Gerente de Finanzas	Sisconta -Sucave	1

Plantilla del inventario de perfiles

Objetivo 2: Propuesta de control de accesos

N°	Control
1	Los colaboradores usen con responsabilidades cuando accedan a los activos de información.
2	Los roles y perfiles de los sistemas y aplicaciones este acorde a las funciones de los usuarios.
3	Los proveedores o usuarios externos usen con responsabilidades cuando accedan a los activos de la información.
4	Los colaboradores solo deben manipular los activos de informacion que han sido autorizados por el area de seguridad de información.
5	Las autorizaciones o conformidades deben ser una proceso formal para la habilitacion de acceso en el sistema.
6	Los proveedores o usuarios externos deben aplicar un proceso formal para revisar o usar los documentos secretos, confidenciales y internos.

Controles propuestos

N°	Incidencias	Descripcion	Agencia	Fecha	Estado	Control
1	Hurto de Informacion de Proveedores	En la Agencia de la ciudad de Cerro Azul se observo que unos proveedores externos hurtaron informacion de la agencia.	Cerro Azul	9/4/2019	Proceso	Los colaboradores usen con responsabilidades cuando accedan a los activos de información.
2	Acceso a diferentes areas de la financiera	El usuario cuando cambio de area y de cargo, no se le quito los accesos a los sistemas	Rositas	12/1/2019	Vencido	Los roles y perfiles de los sistemas y aplicaciones este acorde a las funciones de los usuarios.

Plantilla donde se ejecutara los controles

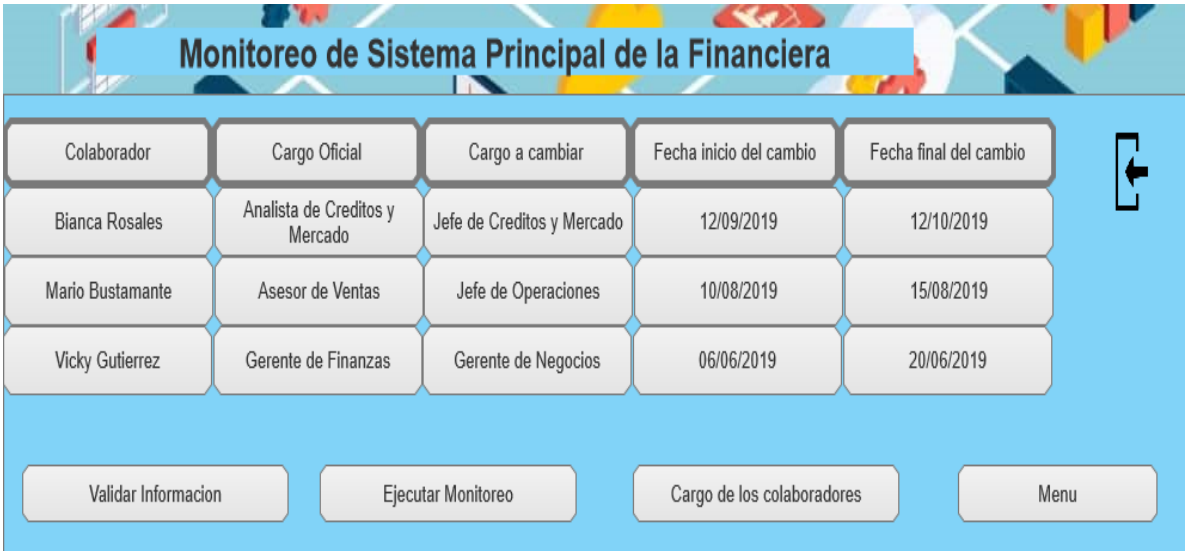
Objetivo 3: Automatización del monitoreo

Colaborador	Cargo Oficial	Cargo a cambiar	Fecha de inicio del cambio	Fecha final de cambio
Blanca Rosales	Analista de Creditos y Mercado	Jefe de Creditos y Mercado	12/09/2019	12/10/2019
Mario Bustamante	Asesor de Ventas	Jefe de Operaciones	10/08/2019	15/08/2019

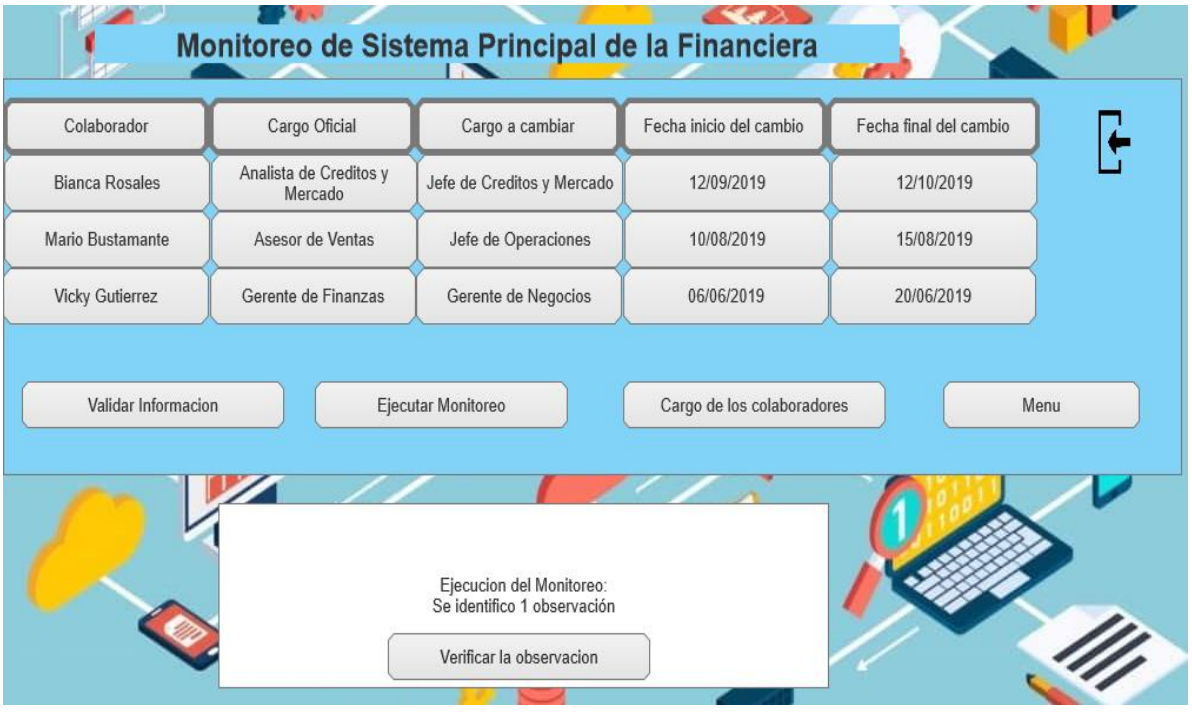
Plantilla de Excel de monitoreo

Login del prototipo

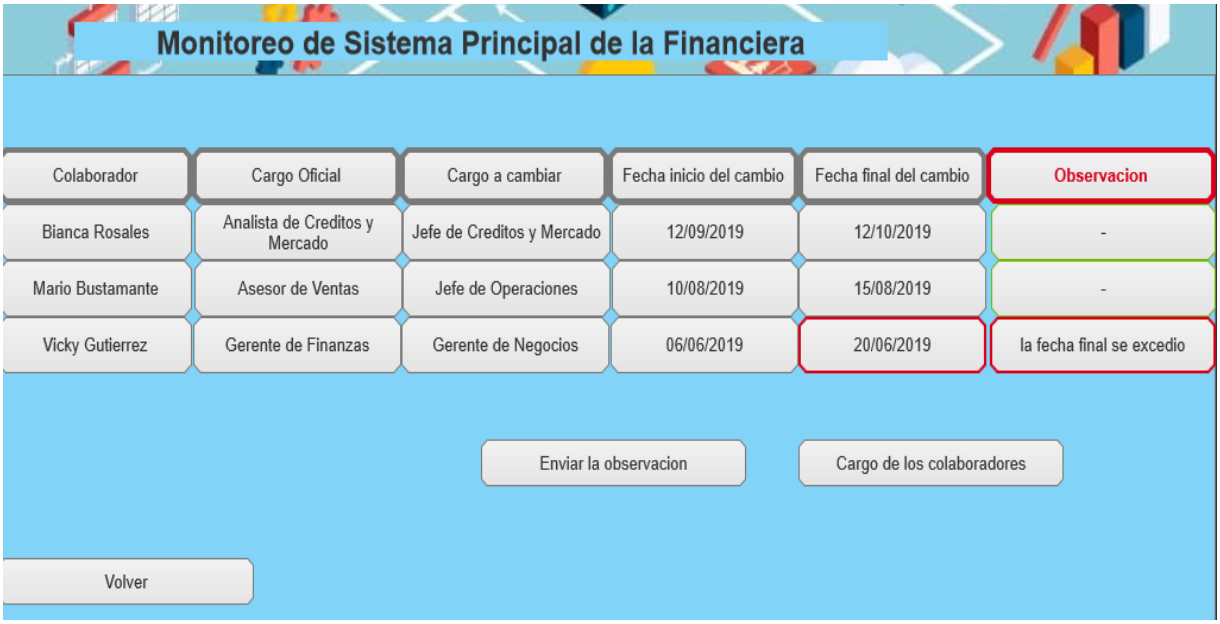
Menú del modelo



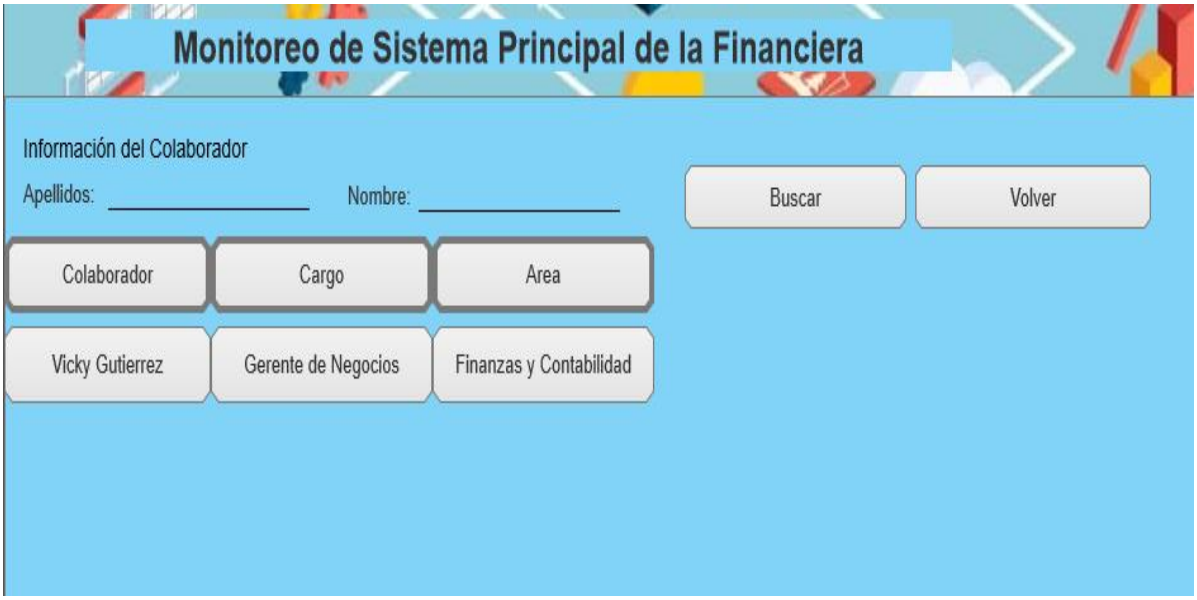
Plantilla de la automatización del monitoreo



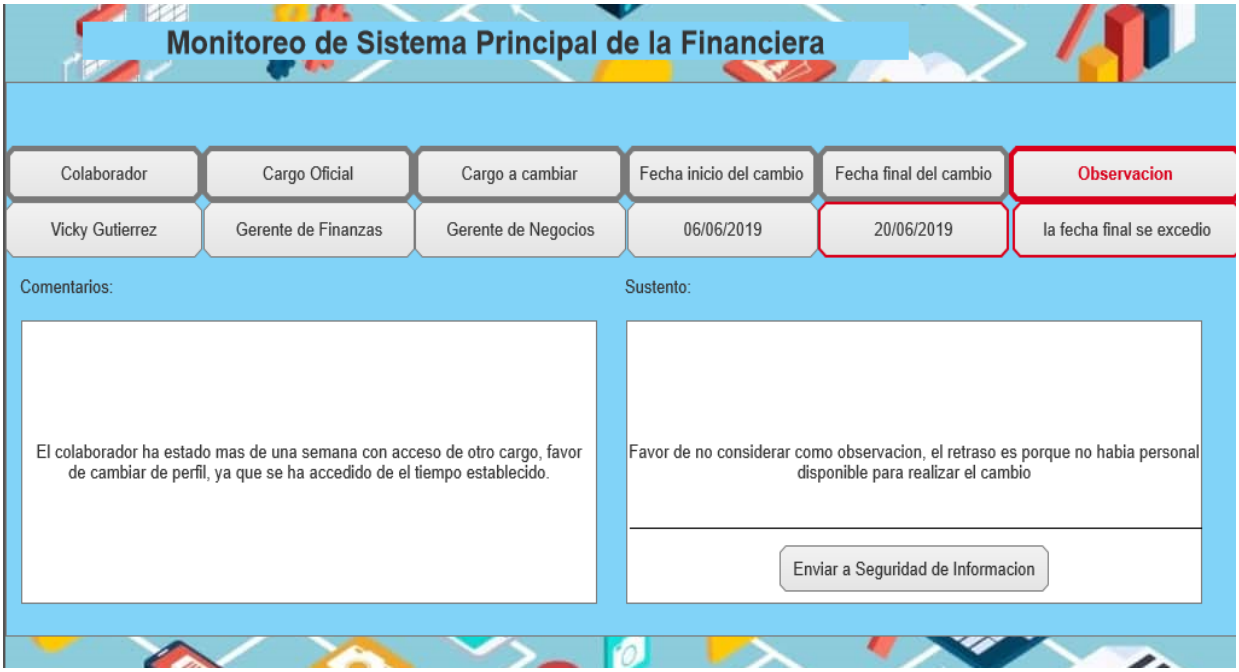
Ejecución del monitoreo



Identificación de la observación



Opción de buscar el cargo del colaborador



El área de Ti sustentando su observación

				Backup				Cargos que interfieren		
N°	Sistemas/Aplicación	Descripcion	Tiempo de recuperacion	Periodo(Diario/Semanal)	Dias que se va almacenar	Almacena	Tipo de respaldo	Analista de Creditos y Mercado	Gerente de Finanzas	Personal externo SBS
1	SUCAVE	Aplicación externa a la acceden a atraves de internet, con un usuario y contraseña	2h	No tiene	-	-	-	x	x	Solicitar Permiso a SI
2	Sisconta	Sistema contanle	2h	Diario	L a V	-	Fisico/Logico	x	x	Solicitar Permiso a SI
3	Sistema Principal	Sistema donde esta los datos de los colaboradores	4h	Diario	L a V	Boveda en la agencia:xx	Fisico/Logico	x	x	Solicitar Permiso a SI

Plantilla del inventario de sistemas

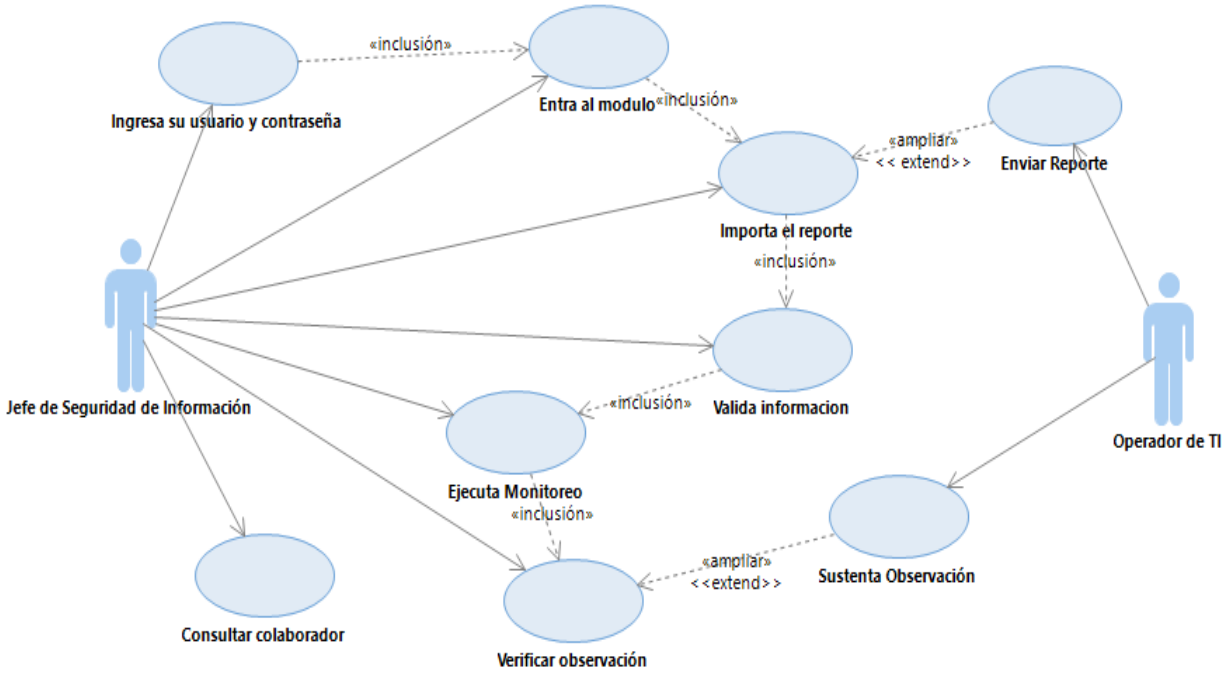


Diagrama de caso de uso de la propuesta

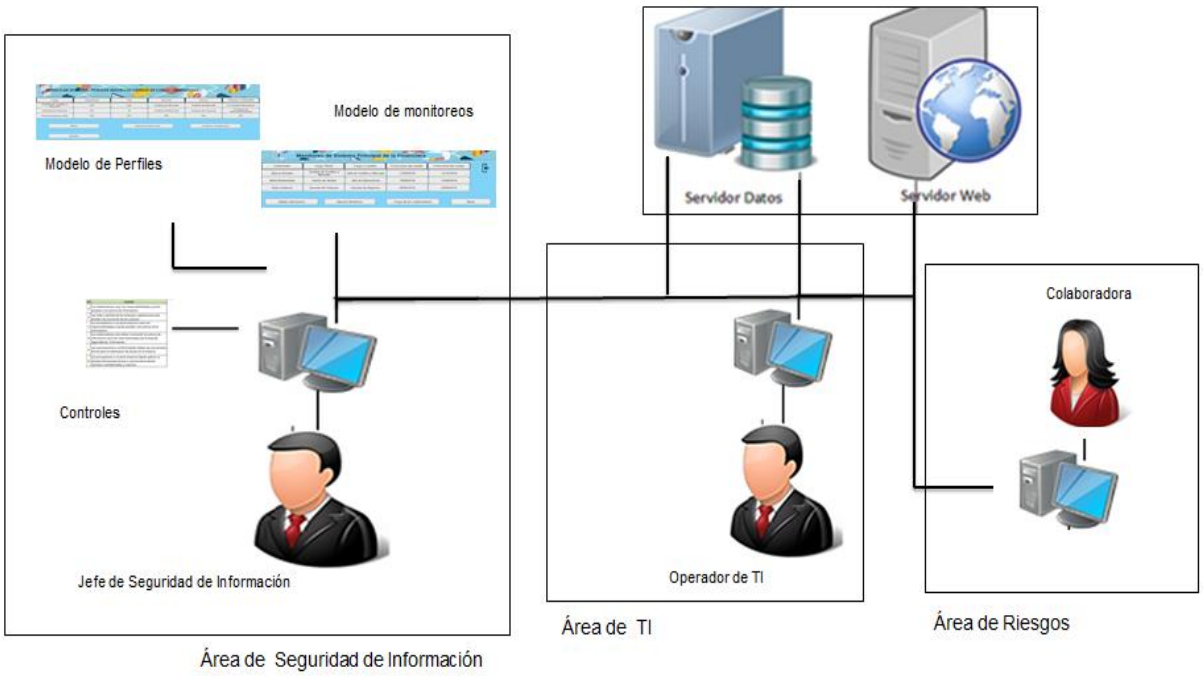


Diagrama Arquitectónico de las propuestas

Conformidad para una implementación de la propuesta.

Prototipo de los objetivos propuestas

Objetivo 1. Modelo de accesos y perfiles

Cargo	TeamViewer	USB	Sisconta	Sucave
Analista de Creditos y Mercado	NO	NO	Analista de Mercado	Analista de Mercado
Gerente de Finanzas	SI	SI	Analista de Mercado	Gerente de Finanzas

Plantilla en Excel modelo de accesos

Login del prototipo

Menú del modelo

Conforme 05/07/19
Frank Manayco
Jefe de Riesgos

Anexo 3: Artículo de investigación

Propuesta de un modelo de control de accesos a los sistemas de información de las financieras

Actualmente, las financieras, corporativas de ahorros y entidades bancarias, tienen incorporada el área de seguridad de información, estando en el departamento de Riesgos, las diversas entidades tienen herramientas y maneras de poder sobrellevar una amenaza dentro de su corporación, hasta alcanzar un plan de acción en el área hacia la corporación.

Accesos en los sistemas de Información

Cuando un colaborador ingresa a una entidad financiera, se le accede a los sistemas de información de la organización, dándole todos los accesos que le corresponde, siendo esto medido por el área de seguridad de información ,ya que cada colaborador debe tener acceso solo a los sistemas que va tener acceso según el cargo que le corresponde, por eso una medida de poder controlar esta medida proponer herramientas automatizadas que puedan analizar, controlar los accesos que usan cada colaborador, teniendo el área de seguridad de información que realizar monitoreo y disponer de controles de seguridad que puedan sobre guardar la información que tiene las entidades financieras a su disposición.

Herramientas Automatizadas

Proponer la implementación de un modelo de control de accesos a los sistemas de información a las financieras de Lima, es poder tener información y conocimiento de la manipulación que realiza cada colaborador dentro y fuera de la entidad financiera. Siendo el objetivo diseñar modelos que puedan ayudar en el funcionamiento del área de seguridad de información en las entidades financieras, cooperativas de ahorro y cajas municipales, en la cual se podrá controlar el manejo y acceso que se le otorga a cada colaborador. De manera que algunas entidades financieras tienen un manejo manual para controlar los accesos de los colaboradores, originando una gran dificultad para controlar los activos de información que tienen en su poder según el cargo que le corresponda en la entidad financiera .Por lo tanto, nace la propuesta de realizar herramientas automatizadas que puedan utilizar el área de seguridad de información, desarrollando prototipos que monitoreen y controlen los perfiles de los colaboradores, en el momento que se le habiliten

los accesos en los sistemas de la entidad financiera. Los prototipos que se va desarrollar va ser manipulado por el área de seguridad de información con la comunicación del área de TI, siendo el área de TI, el encargado de realizar las ejecuciones que ordena y confirma el área de seguridad de información. También con los controles basados a la ISO 27001, se promueve el control de los activos de información y de los colaboradores externos.

Palabras claves: seguridad de información, colaborador, entidad financiera, sistemas, activos de información, controles.

Br. Avalos Cárdenas, Carmen Victoria
vicky41595@gmail.com
Universidad Privada Norbert Wiener
Telf.: 934668667

Anexo 4: Instrumento cuantitativo

CUESTIONARIO DE LA GESTIÓN DE CONTROL DE ACCESOS BASADO EN LA ISO 27001 EN UNA FINANCIERA, LIMA 2019.

INSTRUCCIÓN: Estimado trabajador, este cuestionario tiene como objeto conocer su opinión sobre la gestión de control de accesos basado en la ISO 27001 que se percibe en su centro de trabajo. Dicha información es completamente anónima, por lo que le solicito responda todas las preguntas con sinceridad, y de acuerdo a sus propias experiencias.

Sexo: Masculino ( ) Femenino ( )

Edad: 25-30 años ( ) 30-35 años ( ) 35 a más ( )

Experiencia Laboral: 5-10 años ( ) 10-15 años ( ) 15 años – a más ( )

Condición de Contrato: Por Honorario ( ) Planilla ( )

INDICACIONES: A continuación, se le presenta una serie de preguntas las cuales deberá Ud. responder, marcando una (x) la respuesta que considera correcta.

1	2	3	4	5
Nunca	A veces	Normalmente	Casi siempre	Siempre

ITEMS	ASPECTOS CONSIDERADOS SUB CATEGORÌA POLITICAS DE ACCESOS	VALORACIÓN				
1	¿Cuándo un trabajador comienza a elaborar y asumir sus funciones se le otorgan sus respectivos usuarios al sistema de la financiera?	1	2	3	4	5
2	¿Solicita permisos para ingresar a información secreta, confidencial e interna que no tiene que ver con su cargo?	1	2	3	4	5
3	¿Los colaboradores cumplen con los controles de acceso de seguridad cuando manejan la información de los clientes?	1	2	3	4	5

4	¿Considera Ud. que la financiera cumple con las políticas de seguridad de información para salvaguardar la información?	1	2	3	4	5
5	¿Considera Ud. que los accesos que se le otorgan a los colaboradores tengan restricciones de seguridad?	1	2	3	4	5
6	¿Que la información que usas tienen controles de seguridad en los sistemas y aplicaciones de la empresa?	1	2	3	4	5
7	¿Cuándo se le otorga acceso a los jefes y los proveedores crees que se le debe restringir los accesos que no están a su cargo?	1	2	3	4	5
SUB CATEGORÌA CONTROL DE ACCESOS						
8	¿Ha recibido alguna documentación donde se comprometa a usar con responsabilidad la información que maneja y usa en el sistema de la empresa?	1	2	3	4	5
9	¿Los proveedores cuando inician un contrato con la financiera firman un contrato de confiabilidad?	1	2	3	4	5
10	¿Cuándo se le otorga acceso a los colaboradores se requiere de alguna conformidad del jefe o gerente encargado?	1	2	3	4	5
11	¿Cuándo comparten documentos confidenciales a proveedores o a la SBS, se requiere de conformidad del jefe o gerente?	1	2	3	4	5
12	¿Ha recibido inducción sobre el manejo de la información cuando accede al sistema de la empresa?	1	2	3	4	5
13	¿Considera Ud. que se debería orientar a los colaboradores acerca de las responsabilidades que tiene el usuario cuando usa información de la empresa?	1	2	3	4	5
SUB CATEGORÌA SISTEMAS Y APLICACIONES						
14	¿Todos los sistemas que usa el colaborador tienen definidos los roles y perfiles según los cargos que tiene?	1	2	3	4	5
15	¿Los sistemas que manejan los colaboradores tienen un usuario clave y contraseña?	1	2	3	4	5
16	¿Considera ud. Que los controles no automatizados que tienen la empresa son de utilidad para verificar los accesos indebidos?	1	2	3	4	5
17	¿ Para obtener accesos a los sistemas y aplicaciones que no están asignados según mi cargo, se requiere de la autorización de mi jefe o gerente?	1	2	3	4	5
18	¿Se realiza un adecuado monitoreo de los accesos que se le otorgan a los colaboradores de la empresa?	1	2	3	4	5
19	¿Ha observado ciertas irregularidades en el momento que los colaboradores usen la información de los clientes?	1	2	3	4	5
20	¿Recibe la empresa un informe diariamente?	1	2	3	4	5

Anexo 5: Instrumento cualitativo

Ficha de entrevista

Datos básicos:

Cargo o puesto en que se desempeña	
Nombres y apellidos	
Código de la entrevista	Entrevistado1 (Entv.1)
Fecha	
Lugar de la entrevista	

Nro.	Preguntas de la entrevista
1	¿Cómo es el proceso para que los colaboradores tengan sus accesos en el sistema, y que se requiere para obtener la disponibilidad de información que no tiene a su cargo?
2	¿Qué realiza el área de seguridad de información para que la financiera y los colaboradores cumplan con las políticas de seguridad?
3	¿La empresa como controla los accesos del colaborador y de los proveedores cuando usa la información y como definen Uds. La restricciones que debe tener cada cargo?
4	¿Por qué se considera necesario que los colaboradores y proveedores firmen el compromiso de confiabilidad de información?
5	¿En qué momento se solicitad conformidad para tener accesos a los sistemas?
6	¿Cuáles son los temas que exponen en la inducción a los colaboradores y a que personal de la financiera orienta sobre seguridad de información?
7	¿Cómo definen Uds. qué rol le corresponde al perfil que tiene uso el colaborador en el sistema de la empresa?
8	¿Cuáles son las controles de acceso a los sistemas y aplicaciones que maneja el área y que pasos tiene que seguir para tener accesos a otra sistema que no está a mi cargo?
9	¿Qué beneficios tendría la financiera si usa herramientas para monitorear el control de accesos de la empresa?

Anexo 6: Base de datos (instrumento cuantitativo)

En este cuadro esta las respuestas de los 30 colaboradores con la que se contrasta con las 20 preguntas que se formuló.

PM	1	2	3	4	5	6	7	8	9	10	11	12	13	*14*	15	16	17	18	*19*	20
1	3	1	4	4	1	5	5	5	5	5	5	3	5	2	4	4	5	4	3	3
2	4	4	2	3	3	4	5	4	5	5	4	2	5	2	4	2	5	4	3	3
3	4	5	1	4	3	3	5	4	4	5	4	4	5	3	4	4	5	4	4	4
4	3	3	2	2	2	2	5	2	2	3	3	3	5	2	2	2	3	2	2	3
5	3	1	3	2	3	3	3	1	1	3	3	3	3	3	3	1	3	3	1	3
6	3	1	3	2	4	4	4	1	3	3	3	2	4	2	3	3	3	4	4	3
7	4	1	2	4	5	5	1	5	5	5	4	5	5	5	5	3	5	3	4	4
8	2	1	1	4	5	5	5	5	5	5	5	5	5	4	5	2	5	4	2	4
9	3	2	3	3	3	3	5	3	5	4	4	4	4	3	3	3	3	3	3	5
10	3	1	4	4	4	3	3	4	5	5	4	4	5	2	5	2	4	3	3	3
11	3	4	2	3	3	2	5	2	2	3	3	3	3	3	3	2	3	3	2	4
12	5	5	4	4	4	4	5	5	5	1	3	5	4	2	3	5	4	4	5	3
13	5	1	3	4	4	4	5	1	3	4	4	4	5	2	5	4	4	4	3	4
14	1	1	2	3	5	5	3	1	3	3	3	5	5	3	3	3	3	2	2	4
15	5	1	2	4	1	4	3	2	4	5	4	4	5	2	5	2	2	2	4	3
16	5	1	1	4	1	4	1	3	4	3	1	4	4	1	4	3	2	5	5	3
17	3	4	1	3	1	3	2	5	4	3	3	4	3	2	4	4	3	2	3	3
18	2	4	2	3	2	3	2	5	4	3	3	4	3	4	3	3	3	1	4	3
19	3	2	2	3	1	3	2	3	4	3	3	4	3	2	3	3	2	2	2	3
20	4	1	2	2	3	4	3	3	4	3	1	4	3	3	3	3	4	1	3	3
21	5	4	3	2	2	4	3	4	5	4	1	5	4	2	4	2	3	3	4	4
22	2	5	3	2	2	4	1	4	4	4	2	5	4	2	5	4	2	3	3	4
23	2	2	3	4	3	5	1	4	4	4	3	3	4	1	4	4	1	2	3	4
24	3	2	1	4	2	2	2	4	5	4	2	3	4	1	5	2	2	3	2	3
25	3	3	3	4	1	2	2	4	3	3	2	3	4	2	3	3	3	2	3	3
26	4	3	3	2	1	3	2	5	3	3	3	2	5	3	3	4	3	1	2	5
27	5	4	2	2	3	2	2	3	3	3	3	5	5	3	3	2	4	1	4	5
28	3	4	1	3	3	2	3	3	4	5	3	4	4	2	3	4	4	3	2	3
29	3	5	1	3	1	5	2	3	4	5	1	5	4	1	4	4	3	2	4	3
30	3	4	3	3	2	2	1	3	5	5	2	2	5	2	4	3	4	2	2	4

Anexo 7: Transcripción de las entrevistas o informe del análisis documental

Nro.	Preguntas de la entrevista	Respuestas
1	¿Cómo es el proceso para que los colaboradores tengan sus accesos en el sistema, y que se requiere para obtener la disponibilidad de información que no tiene a su cargo?	Se establecen matrices de roles que permiten definir el tipo de acceso que debe tener cada usuario. Cada rol o perfil a asignar obedecerá a lo indicado por RR.HH. Para acceder a información que no tiene a su cargo es necesario conformidad de su jefatura o gerencia mediante aprobación de seguridad de la información.
2	¿Qué realiza el área de seguridad de información para que la financiera y los colaboradores cumplan con las políticas de seguridad?	Mensajes de correo donde se realiza difusiones mensualmente en la empresa y cursos de capacitación a los colaboradores para que mejoren la concienciación del personal laboral con respecto a la seguridad que tienen que tener por la información que siempre manejan en su entorno laboral.
3	¿La empresa como controla los accesos del colaborador y de los proveedores cuando usa la información y como definen Uds. La restricciones que debe tener cada cargo?	Se controlan mediante matrices de roles definidas en caso de proveedores se establece una documentación de tratamiento de la información previa donde el colaborador o los proveedores detallan y dan a conocer los puntos o medidas implementadas para el manejo de la información.
4	¿Por qué se considera necesario que los colaboradores y proveedores firmen el compromiso de confiabilidad de información?	Si se requiere necesario que los colaboradores y los proveedores firmen un documento donde se comprometan usar con responsabilidad, para evitar fuga de información sensible que pueda perjudicar a la empresa.
5	¿En qué momento se solicitad conformidad para tener accesos a los sistemas?	Se solicita conformidad, cuando el usuario lo requiera, mediante una conformidad de su jefe o gerencia, puede ser para instalar un programa, para cambiar de perfil en los sistemas, entre otros.
6	¿Cuáles son los temas que exponen en la inducción a los colaboradores y a que personal de la financiera orienta sobre seguridad de información?	Los temas pueden ser tratamiento de la información en general y temas relacionados a la seguridad ante amenazas informáticas. Esto está dirigido a todo el personal de la entidad financiera, mas a las personas que usan información confidencial de la empresa.
7	¿Cómo definen Uds. qué rol le corresponde al perfil que tiene uso el colaborador en el sistema de la empresa?	Esto lo define RR.HH., de acuerdo al perfil que está buscando al área solicitante al según el cargo, si es un cargo nuevo se le incorpora las matrices de roles ya establecidas, si es un cargo establecido se le asigna el cargo según la matriz.
8	¿Cuáles son las controles de acceso a los sistemas y aplicaciones que maneja el área y que pasos tiene que seguir para tener accesos a otra sistema que no está a mi cargo?	Los controles que se le otorgan al colaborador se debe detallar según la matriz de roles, los pasos es una conformidad de RR.HH, claro con el visto bueno de seguridad de información y con la autorización del jefe encargado, ya que el área de seguridad da conocer los puntos o medidas implementadas para el manejo de la información que va tener el colaborador, ya que esto es según el cargo o los acceso que va tener el colaborador.
9	¿Qué beneficios tendría la financiera si usa herramientas para monitorear el control de accesos de la empresa?	Si es bueno el uso de herramientas, ya que el uso de estas herramientas podría monitorear los accesos que tienen los colaboradores nuevos, antiguos, y se podría ver si los cesados tienen bloqueado sus accesos.

Anexo 8: Fichas de validación de los instrumentos cuantitativos

Universidad Norbert Wiener

Facultad de Ingeniería y Negocios

Ficha de validez del cuestionario para medir la gestión de control de accesos basado en la ISO 27001 en una Financiera, Lima 2019.

Nro	Items	Suficiencia: Importancia y congruencia del ítem. 1	2	3	4	Pje	Claridad: Ítem adecuado en forma y fondo. 1	2	3	4	Pje	Coherencia: Relación del ítem con el indicador, sub categoría y categoría 1	2	3	4	Pje	Relevancia: Importancia y solidez del ítem. 1	2	3	4	Pje	Observaciones: Si el ítem no cumple con los criterios indicar las observaciones
Sub categoría 1: Políticas de Accesos																						
Indicador 1:Disponibilidad																						
1.	¿Cuándo un trabajador comienza a elaborar y asumir sus funciones se le otorgan sus respectivos usuarios al sistema de la financiera?					4					4					4					4	
2.	¿Solicita permisos para ingresar a información secreta, confidencial e interna que no tiene que ver con su cargo?					4					4					4					4	
Indicador 2:Seguridad																						
3.	¿Los colaboradores cumplen con los controles de acceso de seguridad cuando manejan la información de los clientes?					4					4					4					4	
4.	¿Considera Ud. que la financiera cumple con las políticas de seguridad de información para salvaguardar la información ?					4					4					4					4	
Indicador 3:Accesos de Seguridad																						
5.	¿Considera Ud. que los accesos que se le otorgan a los colaboradores tengan restricciones de seguridad?					4					4					4					4	
6.	¿Que la información que usas tienen controles de seguridad en los sistemas y aplicaciones de la empresa?					4					4					4					4	
7.	¿Cuándo se le otorga acceso a los jefes y los proveedores crees que se le debe restringir los accesos que no están a su cargo?					4					4					4					4	

Nro	Items	Suficiencia: Importancia y congruencia del ítem. 1	2	3	4	Pje	Claridad: Ítem adecuado en forma y fondo. 1	2	3	4	Pje	Coherencia: Relación del ítem con el indicador, sub categoría y categoría 1	2	3	4	Pje	Relevancia: Importancia y solidez del ítem. 1	2	3	4	Pje	Observaciones: Si el ítem no cumple con los criterios indicar las observaciones
Sub categoría 2: Control de Accesos																						
Indicador 4:Compromiso con los colaboradores																						
8.	¿Ha recibido alguna documentación donde se comprometa a usar con responsabilidad la información que maneja y usa en el sistema de la empresa?					4					4					4					4	
9.	¿Los proveedores cuando inician un contrato con la financiera firman un contrato de confiabilidad?					4					4					4					4	
Indicador 5:Medidas de Acceso																						
10.	¿Cuándo se le otorga acceso a los colaboradores se requiere de alguna conformidad del jefe o gerente encargado?					4					4					4					4	
11.	¿Cuándo comparten documentos confidenciales a proveedores o a la SBS, se requiere de conformidad del jefe o gerente?					4					4					4					4	
Indicador 6:Induccion																						
12.	¿Ha recibido inducción sobre el manejo de la información cuando accede al sistema de la empresa?					4					4					4					4	
13.	¿Considera Ud. que se debería orientar a los colaboradores acerca de las responsabilidades que tiene el usuario cuando usa información de la empresa?					4					4					4					4	
Sub categoría 3: Sistemas y Aplicaciones																						
Indicador 7: Uso																						
14.	¿Todos los sistemas que usa el colaborador tienen definidos los roles y perfiles según los cargos que tiene?					4					4					4					4	
15.	¿Los sistemas que manejan los colaboradores tienen un usuario clave y contraseña?					4					4					4					4	

Indicador 8:Acceso																																	
16.	¿Considera Ud. que los controles no automatizados que tienen la empresa son de utilidad para verificar los accesos indebidos?						4						4						4						4						4		
17.	¿ Para obtener accesos a los sistemas y aplicaciones que no están asignados según mi cargo, se requiere de la autorización de mi jefe o gerente?						4						4						4						4						4		
Indicador 9: Monitoreo																																	
18.	¿Se realiza un adecuado monitoreo de los accesos que se le otorgan a los colaboradores de la empresa?						4						4						4						4						4		
19.	¿Ha observado ciertas irregularidades en el momento que los colaboradores usen la información de los clientes?						4						4						4						4						4		
20.	¿Recibe la empresa un informe diariamente?						4						4						4						4						4		

Validado por:

Apellidos	Chávez Alvarado, G		
Nombres	Walter Armando		
Profesión	Ingeniero de Sistemas		
Máximo grado obtenido	Magister		
Especialidad			
Años de experiencia	20 años		
Cargo que desempeña actualmente	Docente tiempo Parcial	DNI:	09791774
		Sello y firma:	
Fecha	17-04-2019		

Universidad Norbert Wiener

Facultad de Ingeniería y Negocios

Ficha de validez del cuestionario para medir la gestión de control de accesos basado en la ISO 27001 en una Financiera, Lima 2019.

Nro	Items	Suficiencia					Claridad					Coherencia					Relevancia					Observaciones
		Importancia y congruencia del ítem.					Ítem adecuado en forma y fondo.					Relación del ítem con el indicador, sub categoría y categoría					Importancia y solidez del ítem.					Si el ítem no cumple con los criterios indicar las observaciones
Sub categoría 1: Políticas de Accesos		1	2	3	4	Pje	1	2	3	4	Pje	1	2	3	4	Pje	1	2	3	4	Pje	
Indicador 1:Disponibilidad																						
1.	¿Cuándo un trabajador comienza a elaborar y asumir sus funciones se le otorgan sus respectivos usuarios al sistema de la financiera?	El ítem no es suficiente para medir la sub categoría o indicador.	No existe relación entre el ítem, sub categoría e indicador.	Es necesario incrementar los ítems.	Es suficiente el número de ítems, son congruentes con las	4	El ítem requiere modificaciones en base al marco conceptual.	La redacción del ítem no es clara/entendible.	Es necesaria la modificación del ítem.	El ítem es claro, tiene semántica y es adecuado.	4	No existe coherencia entre la categoría, sub categoría, indicador e	Existe escasa relación entre la categoría, sub categoría, indicador e	Existe regular relación entre la categoría, sub categoría, indicador e	Existe relación alta y exigida entre la categoría, sub categoría, indicador	4	La eliminación del ítem no afecta al indicador, subcategoría o categoría.	El ítem no mide de manera relevante el indicador, subcategoría y	El ítem requiere aún modificaciones para ser relevante.	El ítem es relevante y debe ser incluido en el instrumento.	4	
2.	¿Solicita permisos para ingresar a información secreta, confidencial e interna que no tiene que ver con su cargo?					4					4					4					4	
Indicador 2:Seguridad																						
3.	¿Los colaboradores cumplen con los controles de acceso de seguridad cuando manejan la información de los clientes?					4					4					4					4	
4.	¿Considera Ud. que la financiera cumple con las políticas de seguridad de información para salvaguardar la información ?					4					4					4					4	
Indicador 3:Accesos de Seguridad																						
5.	¿Considera Ud. que los accesos que se le otorgan a los colaboradores tengan restricciones de seguridad?					4					4					4					4	
6.	¿Que la información que usas tienen controles de seguridad en los sistemas y aplicaciones de la empresa?					4					4					4					4	
7.	¿Cuándo se le otorga acceso a los jefes y los proveedores crees que se le debe restringir los accesos que no están a su cargo?					4					4					4					4	

Nro	Items	Suficiencia: Importancia y congruencia del ítem.					Claridad: Ítem adecuado en forma y fondo.					Coherencia: Relación del ítem con el indicador, sub categoría y categoría					Relevancia: Importancia y solidez del ítem.					Observaciones: Si el ítem no cumple con los criterios indicar las observaciones
		1	2	3	4	Pje	1	2	3	4	Pje	1	2	3	4	Pje	1	2	3	4	Pje	
Sub categoría 2: Control de Accesos																						
Indicador 4:Compromiso con los colaboradores																						
8.	¿Ha recibido alguna documentación donde se comprometa a usar con responsabilidad la información que maneja y usa en el sistema de la empresa?					4					4					4					4	
9.	¿Los proveedores cuando inician un contrato con la financiera firman un contrato de confiabilidad?					4					4					4					4	
Indicador 5:Medidas de Acceso																						
10.	¿Cuándo se le otorga acceso a los colaboradores se requiere de alguna conformidad del jefe o gerente encargado?					4					4					4					4	
11.	¿Cuándo comparten documentos confidenciales a proveedores o a la SBS, se requiere de conformidad del jefe o gerente?					4					4					4					4	
Indicador 6:Induccion																						
12.	¿Ha recibido inducción sobre el manejo de la información cuando accede al sistema de la empresa?					4					4					4					4	
13.	¿Considera Ud. que se debería orientar a los colaboradores acerca de las responsabilidades que tiene el usuario cuando usa información de la empresa?					4					4					4					4	
Sub categoría 3: Sistemas y Aplicaciones																						
Indicador 7: Uso																						
14.	¿Todos los sistemas que usa el colaborador tienen definidos los roles y perfiles según los cargos que tiene?					4					4					4					4	
15.	¿Los sistemas que manejan los colaboradores tienen un usuario clave y contraseña?					4					4					4					4	

Indicador 8:Acceso																						
16.	¿Considera Ud. que los controles no automatizados que tienen la empresa son de utilidad para verificar los accesos indebidos?					4					4					4					4	
17.	¿ Para obtener accesos a los sistemas y aplicaciones que no están asignados según mi cargo, se requiere de la autorización de mi jefe o gerente?					4					4					4					4	
Indicador 9: Monitoreo																						
18.	¿Se realiza un adecuado monitoreo de los accesos que se le otorgan a los colaboradores de la empresa?					4					4					4					4	
19.	¿Ha observado ciertas irregularidades en el momento que los colaboradores usen la información de los clientes?					4					4					4					4	
20.	¿Recibe la empresa un informe diariamente?					4					4					4					4	

Validado por:

Apellidos	Fox Cortez.		
Nombres	Julio Alonso		
Profesión	Catedratico		
Máximo grado obtenido	Doctor		
Especialidad	Educacion		
Años de experiencia	30		
Cargo que desempeña actualmente	Docente Tiempo Completo	DNI:	25602115
Fecha	7-04-14	Sello y firma:	

Universidad Norbert Wiener

Facultad de Ingeniería y Negocios

Ficha de validez del cuestionario para medir la gestión de control de accesos basado en la ISO 27001 en una Financiera, Lima 2019.

Nro	Items	Suficiencia: Importancia y congruencia del ítem.					Claridad: Ítem adecuado en forma y fondo.					Coherencia: Relación del ítem con el indicador, sub categoría y categoría					Relevancia: Importancia y solidez del ítem.					Observaciones: Si el ítem no cumple con los criterios indicar las observaciones
		1	2	3	4	Pje	1	2	3	4	Pje	1	2	3	4	Pje	1	2	3	4	Pje	
Sub categoría 1: Políticas de Accesos																						
Indicador 1:Disponibilidad																						
1.	¿Cuándo un trabajador comienza a elaborar y asumir sus funciones se le otorgan sus respectivos usuarios al sistema de la financiera?	El ítem no es suficiente para medir la sub categoría o indicador.	No existe relación entre el ítem, sub categoría e indicador.	Es necesario incrementar los ítems.	Es suficiente el número de ítems, son congruentes con las	4	La redacción del ítem no es clara/redundante.	El ítem requiere modificaciones en base al marco conceptual.	Es necesaria la modificación del ítem.	El ítem es claro, tiene semántica y es adecuado.	4	No existe coherencia entre la categoría, indicador e	Existe escasa relación entre la categoría, indicador e	Existe regular relación entre la categoría, indicador e	Existe relación alta y exigida entre la categoría, sub categoría, indicador	4	La eliminación del ítem no afecta al indicador, subcategoría o categoría.	El ítem no mide de manera relevante el indicador, subcategoría y	El ítem requiere aún modificaciones para ser relevante.	El ítem es relevante y dee ser incluido en el instrumento.	4	
2.	¿Solicita permisos para ingresar a información secreta, confidencial e interna que no tiene que ver con su cargo?					4					4					4					4	
Indicador 2:Seguridad																						
3.	¿Los colaboradores cumplen con los controles de acceso de seguridad cuando manejan la información de los clientes?					4					4					4					4	
4.	¿Considera Ud. que la financiera cumple con las políticas de seguridad de información para salvaguardar la información ?					4					4					4					4	
Indicador 3:Accesos de Seguridad																						
5.	¿Considera Ud. que los accesos que se le otorgan a los colaboradores tengan restricciones de seguridad?					4					4					4					4	
6.	¿Que la información que usas tienen controles de seguridad en los sistemas y aplicaciones de la empresa?					4					4					4					4	
7.	¿Cuándo se le otorga acceso a los jefes y los proveedores crees que se le debe restringir los accesos que no están a su cargo?					4					4					4					4	

Nro	Items	Suficiencia: Importancia y congruencia del ítem.					Claridad: Ítem adecuado en forma y fondo.					Coherencia: Relación del ítem con el indicador, sub categoría y categoría					Relevancia: Importancia y solidez del ítem.					Observaciones: Si el ítem no cumple con los criterios indicar las observaciones
		1	2	3	4	Pje	1	2	3	4	Pje	1	2	3	4	Pje	1	2	3	4	Pje	
Sub categoría 2: Control de Accesos																						
Indicador 4:Compromiso con los colaboradores																						
8.	¿Ha recibido alguna documentación donde se comprometa a usar con responsabilidad la información que maneja y usa en el sistema de la empresa?	El ítem no es suficiente para medir la sub categoría o indicador.	No existe relación entre el ítem, sub categoría e indicador.	Es necesario incrementar los ítems.	Es suficiente el número de ítems, son congruentes con las subcategorías y la categoría.	4	La redacción del ítem no es clara/redundante.	El ítem requiere modificaciones en base al marco conceptual.	Es necesaria la modificación del ítem.	El ítem es claro, tiene semántica y es adecuado.	4	No existe coherencia entre la categoría, indicador e ítems.	Existe escasa relación entre la categoría, sub categoría, indicador e ítems.	Existe regular relación entre la categoría, sub categoría, indicador e ítems.	Existe relación alta y exigida entre la categoría, sub categoría, indicador e ítems.	4	La eliminación del ítem no afecta al indicador, subcategoría o categoría.	El ítem no mide de manera relevante el indicador, subcategoría y categoría.	El ítem requiere aún modificaciones para ser relevante.	El ítem es relevante y dee ser incluido en el instrumento.	4	
9.	¿Los proveedores cuando inician un contrato con la financiera firman un contrato de confiabilidad?					4					4					4					4	
Indicador 5:Medidas de Acceso																						
10.	¿Cuándo se le otorga acceso a los colaboradores se requiere de alguna conformidad del jefe o gerente encargado?					4					4					4					4	
11.	¿Cuándo comparten documentos confidenciales a proveedores o a la SBS, se requiere de conformidad del jefe o gerente?					4					4					4					4	
Indicador 6:Induccion																						
12.	¿Ha recibido inducción sobre el manejo de la información cuando accede al sistema de la empresa?					4					4					4					4	
13.	¿Considera Ud. que se debería orientar a los colaboradores acerca de las responsabilidades que tiene el usuario cuando usa información de la empresa?					4					4					4					4	
Sub categoría 3: Sistemas y Aplicaciones																						
Indicador 7: Uso																						
14.	¿Todos los sistemas que usa el colaborador tienen definidos los roles y perfiles según los cargos que tiene?					4					4					4					4	
15.	¿Los sistemas que manejan los colaboradores tienen un usuario clave y contraseña?					4					4					4					4	

Indicador 8:Acceso																															
16.	¿Considera Ud. que los controles no automatizados que tienen la empresa son de utilidad para verificar los accesos indebidos?	El ítem no es suficiente para medir la sub.	No existe relación entre el ítem, sub	Es necesario incrementar los ítems.	Es suficiente el número de ítems, son	4		La redacción del ítem no es	El ítem requiere modificaciones en base al	Es necesaria la modificación del ítem		4		No existe coherencia entre la categoría, sub.	Existe escasa relación entre la categoría,	Existe regular relación entre la categoría,	Existe relación alta y exigida entre la			La eliminación del ítem no afecta al	El ítem no mide de manera relevante el	El ítem requiere aún modificaciones para	El ítem es relevante y dee ser incluido en el	4						
17.	¿ Para obtener accesos a los sistemas y aplicaciones que no están asignados según mi cargo, se requiere de la autorización de mi jefe o gerente?					4						4											4							
Indicador 9: Monitoreo																															
18.	¿Se realiza un adecuado monitoreo de los accesos que se le otorgan a los colaboradores de la empresa?					4						4											4							
19.	¿Ha observado ciertas irregularidades en el momento que los colaboradores usen la información de los clientes?					4						4											4							
20.	¿Recibe la empresa un informe diariamente?					4						4											4							

Validado por:

Apellidos	RAMOS MUÑOZ	
Nombres	ALFREDO MARINO	
Profesión	INGENIERO	
Máximo grado obtenido	MAGISTER	
Especialidad	TECNOLOGIA DE LA INFORMACION	
Años de experiencia	25 AÑOS	
Cargo que desempeña actualmente	GERENTE - CONSULTOR	DNI: 07567647
Fecha		Sello y firma:

Anexo 9: Evidencia de la visita a la empresa

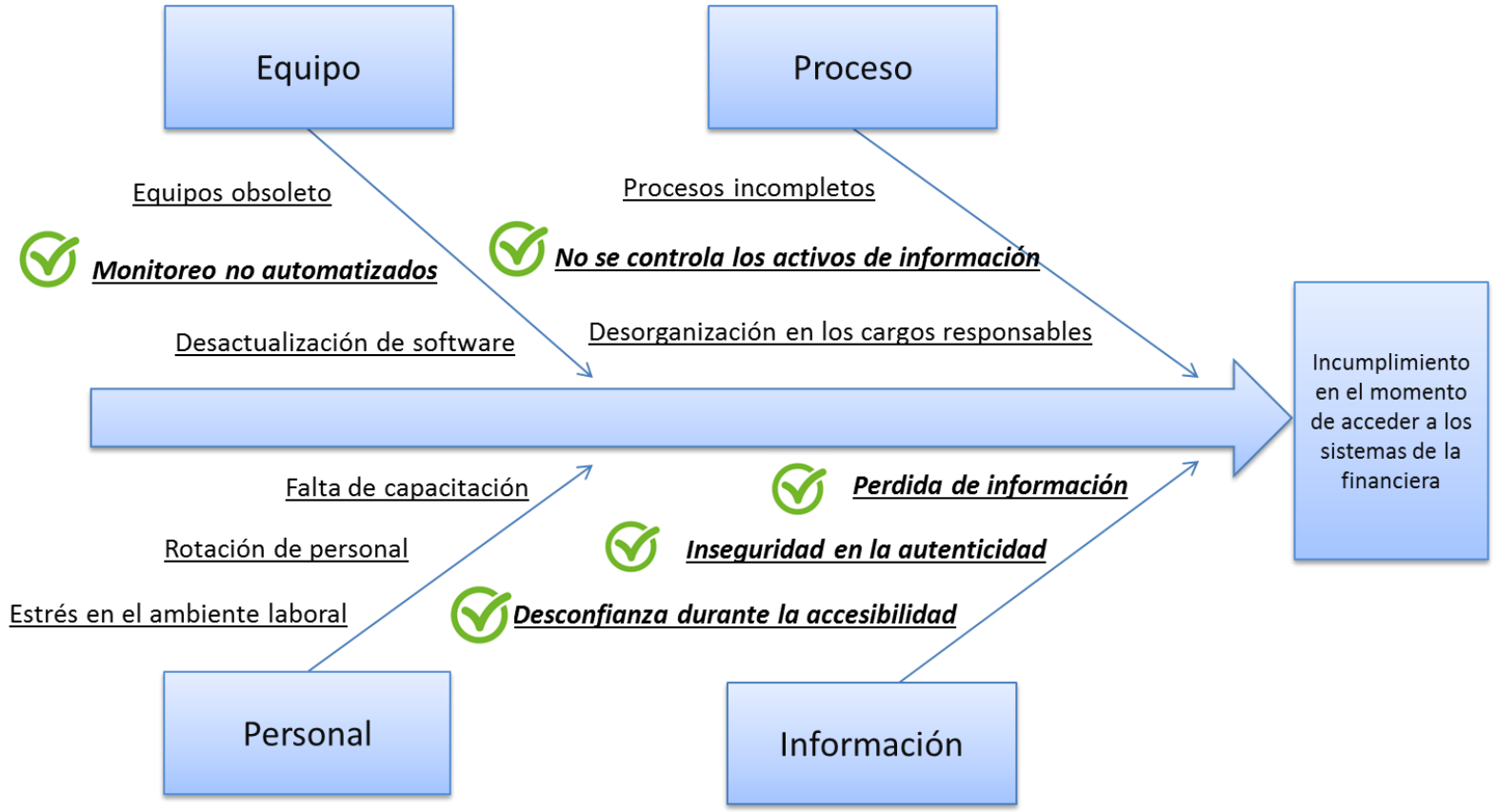
Área Interna de Financiera Credinka

Anexo 10: Matrices de trabajo

1. Matriz de causa efecto para definir el problema

Causa	Sub causa	¿Por qué?	Efecto (Categoría problema)
C1. Personal	1. Falta de capacitación	1. Incumplimiento en la protección de información.	Gestión de Control de Accesos
		2. No tienen orientación sobre las políticas de escritorio limpio y las buenas practicas	
	2. Ambiente laboral	3. Mantienen un ambiente estresante	
		4. No hay un ambiente seguro para el resguardo de su información.	
	3. Rotación de personal	5. Pierde la confianza de mantener la información a una sola persona	
		6. No va tener conocimiento de las normas que tiene que seguir para mantener una información segura	
C2. Equipos	4. Equipos obsoleto	7. El servidor que resguarda la información, se puede dañar en cualquier momento	
		8. No hay presupuesto del área	
	5. Desactualización de software	9. Habrá problema en las restricciones de sus perfiles en el sistema en el momento de acceder a los documentos	
		10. Los colaboradores que tienen prohibido la información podrá acceder a información confiable.	
	6. Monitoreo	11. Control de los accesos de información a los usuarios	
		12. No tendrá un control remoto sobre el uso que tendrá dicha información	
C3. Procesos	7. Procesos incompleta	13. No hay control de cambios de las actividades y/o tareas que interviene información (reservada, secreta e interna)	
		14. No tienen una comunicación con las áreas	
	8. Jerarquización en los cargos responsables	15. El colaborador no tendrá conocimiento de sus funciones	
		16. Errores en el manejo de documentación	
	9. Activos de información del área	17. Desactualización de los activos	
		18. No tienen un control de activos que usan en el área.	
C4. Información	10. Perdida de información	19. No habrá un manejo de datos confiables	
		20. Problema de imagen de la empresa	
	11. Autenticidad	21. Errores en los datos personales de los clientes	
		22. Problema de mantener datos seguros	
	12. Accesibilidad	23. Mal uso de la información	
		24. Hurto de la información	

Diagrama de Ishikawa



2. Problema, objetivo, hipótesis

Problema general	Objetivo general
¿Cómo mejorar el control de accesos de los sistemas y aplicaciones en una entidad financiera, 2019?	Proponer controles y herramientas que disminuya el incumplimiento de privacidad de la información en la mejora del proceso de gestión de control de accesos a los sistemas y aplicaciones en las financieras de Lima, 2019.
Problemas específicos	**Objetivos específicos**
¿Cómo es el control de accesos de los sistemas y aplicaciones en una entidad financiera, Lima 2019? ¿Cuáles son las causas de mayor amenaza en los controles de accesos de los sistemas y aplicaciones de una entidad financiera, 2019? ¿Cómo las estrategias influyen en el control de accesos de los sistemas y aplicaciones en una entidad financiera, 2019?	Diagnosticar la posición de la gestión de control de accesos de los sistemas y aplicación en la financiera de Lima, 2019. Explicar las causas de mayor importancia que ocasionan vulnerabilidades en la gestión de control de accesos de los sistemas y aplicaciones en una entidad financiera, 2019 Predecir la influencia de las estrategias en la gestión de control de accesos de los sistemas y aplicaciones en una entidad financiera, 2019.

3. Justificación

Justificación teórica		
Cuestiones	**Respuesta**	**Redacción final**
¿Qué teorías sustentan la investigación?	Sustento la teoría del mosaico, teoría general de sistemas, teoría de la información, teoría de procesamiento de la información y teoría desarrollo organizacional.	Las teorías nos dan un medio de información para poder sustentar la idea que nos va a llevar a una solución.
¿Cómo estas teorías aportan a su investigación?	Define que la información personal que tiene el usuario puede ser alterada o manipulada por terceros.	Están teorías nos aporta información de transacción de datos personales, controles de acceso, el desarrollo que debe tener el colaborador de la entidad financiera cuando tenga al uso la información confidencial que nos brinda el cliente.
Justificación práctica		
¿Por qué hacer el trabajo de investigación?	Al tener seguimiento de los incidentes de protección de datos registrados, nos ayuda a controlar los acechos que podemos identificar durante la manipulación de la información que tiene usuarios.	De acuerdo a los objetivos de estudio de la investigación permite tomar decisiones durante el proceso de solución del proceso de gestión de control de accesos.
¿Cuál será la utilidad?	Para la entidad financiera, medir el control y monitoreo del acceso indebido que se les otorgan a los colaboradores que no tienen acceso a dicha información.	Las entidades Financieras de Lima, que no tengan en su división controles automatizados para reducir el riesgo residual de los controles de gestión de accesos.
¿Qué espera con la investigación?	Controla las vulnerabilidades que se pueden registrar con el robo de información.	Controlar las amenazas internas

Justificación metodológica		
¿Por qué investiga bajo ese diseño?	Permitirá conocer más la gestión de control de accesos en alas entidades Financieras, realizando los métodos determinados.	La investigación permitirá conocer como es la gestión de control de accesos en las entidades Financieras en Lima, realizando los métodos propuestos con la finalidad de realizar y elaborar una propuesta de solución al problema de incumplimiento de control de accesos que tiene los colaboradores en las Financieras de Lima.
¿El resultado de la investigación Permitirá resolver algún problema?	Nos permitirá dar a los clientes la confianza y seguridad cuando nos otorguen la información que nos brinda.	Asimismo, podemos dar un beneficio a los clientes que confían cuando nos brindan su información personal, otorgándoles herramientas y controles para detectar los incumplimientos que tienen los colaboradores en el momento que tienen acceso a la información de la empresa.

4. Matriz de teorías

Teoría 1: Teoría General de Sistemas				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Bertalanffy, L. Von.	1976	Según Bertalanffy (1976) Indica que la "Teoría General de Sistemas": La teoría es el sentido más estricto, que procurar derivar, partiendo de una definición general de "sistemas" como complejo de componentes interactuantes, conceptos característicos de totalidades organizadas, tales como interacción, suma, mecanización, centralización, competencia, finalidad, etc, y aplicarlos entonces en fenómenos concreto (p.94).	Se determina que la teoría tiene una complejidad de componentes para caracterizar información, tácticas, métodos y procedimientos para puntualizar mejores decisiones en los novedosos recursos explicativo e informativos (Bertalanffy, 1976).	Por ello el sistema que se va implementar, va eliminar la vulnerabilidad, debilidades que puede afectar a la corporación y a nuestra división, con las nuevas decisiones se va poder solucionar los problemas o brechas que tiene la división para llegar a una solución.
Referencia:	Bertalanffy, L. (1976). Teoría General de los Sistemas. Mexico: Fondo de Cultura Económica.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Tamayo Alzate, Alonso	1999	Según Tamayo (1999) , con respecto a la teoría general de sistemas mencionó: La Metodología de Sistemas desarrollada y empleada adecuadamente puede mejorar la productividad aumentando el volumen de trabajo realizado, ayudando a las empresas a incrementar sus ganancias, a mejorar su administración y a satisfacer los requerimientos de los usuarios. Como se puede apreciar, se trata de una metodología generalizable, ya que consiste simplemente en una utilización más del método científico (p.3).	Es decir, la implementación de una metodología de sistemas en la empresa, puede enriquecer las ganancias, producción, beneficiando a la empresa a cooperar con la asistencia de los requerimientos que demandan los usuarios (Tamayo, 1999).	En el momento de ser uso de la metodología de sistemas se puede reducir las amenazas críticas que repercute en las actividades de los colaboradores de la empresa, ampliando la imagen corporativa ante el público.
Referencia:	Tamayo, A. (1999). Teoría General de Sistemas. Colombia: Universidad Nacional de Colombia.			

Autor/es	Año	Cita	Parafraseo	Aplicación en su tesis
Luz Arabany Ramirez	2002	Según Arabany (citado por Gigh,2002), opina que la teoría general de sistema es: Un sistema abierto y cerrado, siendo el sistema cerrado es un sistema que no tiene medio, es decir, no hay sistemas externos que lo violen, o a través del cual ningún sistema externo será considerado. Un sistema abierto es aquel que posee medio, es decir, posee otros sistemas con los cuales se relaciona, intercambia y comunica (p.35).	La teoría general de sistemas se define por un sistema abierto y cerrado, teniendo el sistema abierto medio para relacionarse entre otros sistemas, viendo diversas conexiones y transacciones de datos, y el sistema cerrado se define por no tener comunicación o conexión con otro equipo (Arabany, 2002).	Los sistemas que se expresa abierto y cerrado, se puede ver que los diversos sistemas pueden tener transacciones de datos e información teniendo accesos o no accesos a los usuarios.
Referencia:	Arabany Ramirez, L. (2002). Teoría de Sistemas. Colombia: Universidad Nacional de Colombia.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Angel A. Sarabia	1995	Según Sarabia (1995),considera que la teoría general de sistemas tiene: Una percepción dinámica de la realidad como constituida por procesos. Un proceso es todo cambio en el tiempo, pero no forzosamente en función del tiempo, de materia, energía y/o información (p.96).	Expresa que la teoría general de sistemas se ha hecho por medio de procesos, que durante los cambios o rediseño que sufre la organización puede sufrir cambios en la información, en los objetos, y tiempo en las actividades de la organización (Sarabia, 1995).	La teoría define que la dinámica que sufre de los sistemas puede sufrir cambios en los procesos por las funciones que realizan los usuarios o por las necesidades que requiere la persona en momento que usa un sistema.
Referencia:	Sarabia, A. (1995). La Teoría General de Sistemas. España: Isdefe Ingeniería de Sistemas.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Javier Torres Nafarrate	1996	Según Torres (citado por Luhmann, Niklas,1996) considera que la teoría general de sistemas viene: Tomando pie en los estímulos de estos planteamientos, la teoría de sistemas se fue constituyendo ella misma en un sistema de autoobservación, recursivo, circular, autopoiético; dotado de una dinámica intelectual propia y fascinante capaz de estar a la altura de los planteamientos problemáticos que hoy se enuncian bajo la noción de posmodernismo (p.59)	La teoría se ha originado por las diversos cambios que ocurre en los sistemas, ya que los sistemas puede desarrollar diversas actividades, que cambie los labores de los usuarios, para que ellos pueden tomar una buena decisión en el momento que sucede un problema en la época moderna y tecnológicas (Torres, 1996).	Para llevar a cabo cambios en los sistemas, se requiere ver la necesidad para que el líder puede las funciones que requiere, siendo esto necesario, para que pueda asumir responsabilidades y decisiones antes los problemas que se ve en la vida real y profesional.
Referencia:	Torres Nafarrate, J. (1996). Introducción a la teoria de Sistemas. Mexico: Universidad Iberoamericana, A.c			

Teoría 2: Teoría del Mosaico				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Carlos Ruiz Miguel	1994	Según Ruiz (citado por Madrid Conesa, 1994), indica que la Teoría del Mosaico: Esta teoría estima lo privado y lo público como conceptos relativos. De ahí concluye, en primer lugar, que lo privado y lo público son relativos en función de quién sea el otro sujeto en la relación informativa (p.243).	La teoría pronuncia que la información privada y pública, es función que tiene la persona y la utilidad que le da el otro usuario que gestiona la información. De manera que la información sumamente importante debe estar protegida por el hurto y robo de información (Ruiz, 1994).	La teoría nos permite reconocer que la información secreta y confidencial, que manipule el colaborador debe contar con normas de LPD para evitar la mala manipulación de la información que se seta manejando en el ente financiero.
Referencia:	Ruiz, C. (1994). En torno a la protección de los datos personales automatizados. España: Revista de Estudios Políticos. (Vol. 84, págs. 237-264).			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
José Calderón Carrero	2009	Según Calderón (citado por Ruiz Miguel, 2009), la teoría de Mosaicos define: No obstante, como ha puesto de relieve Ruiz Miguel, «existen datos a priori irrelevantes desde el punto de vista del derecho a la intimidad y que, sin embargo, en conexión con otros, quizá también irrelevantes, pueden servir para hacer totalmente transparente la personalidad de un ciudadano» (p.35).	Se determinó que, en los medios de comunicación, pueden existir personas que vulneren y expongan la información personal de otros usuarios, siendo alterada y modificada para beneficios monetarios (Calderón, 2009).	La teoría permite diferenciar las amenazas que se arriesga la persona al subir por medios de comunicación sus datos personales y secretos, siendo una terrible exposición de los usuarios, que puede ser beneficiado por personas que se roban la identidad de otros.
Referencia:	Calderon, J. (2009). El derecho de los contribuyentes al secreto tributario. España: Editorial Netbiblo.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Herrera Carpintero Paloma	2016	Según Herrera (citado por Madrid,1984) la teoría del mosaico consiste: Cada dato recabado a través de las cookies da la posibilidad de revelar la identidad real de las personas, exponiendo datos sensibles del usuario, concernientes a sus gustos, pasatiempos, ideología, entre otros (p.10).	La teoría del mosaico consiste que un usuario cuando envía o guarda información a la red, muestra al mundo y a diferentes personas tu personalidad, poniendo en riesgo tu información personal (Herrera, 2016)	Nuestra investigación consiste en sobre guardar la información de los clientes a través de modelos y estrategias para que nuestros colaboradores tenga un mejor uso de la información.
Referencia:	Herrera, P. (2016). El derecho a la vida privada y las redes sociales en Chile. Chile: Revista Chilena de derecho y tecnología. (Vol. 5, págs. 87-112).			

Autor/es	Año	Cita	Parafraseo	Aplicación en su tesis
Nogueira Alcala Humberto	1998	Según Alcala (1998) define que la teoría del mosaico es: El concepto de vida privada se incluyen también datos que a primera vista pueden ser irrelevantes desde la perspectiva de protección de la privacidad de la persona, pero que, en conexión con otros datos, que también pueden ser, aislados, de carácter irrelevante, considerados en su conjunto pueden hacer totalmente transparente la personalidad de un individuo (p.72).	Podemos ver que la teoría del mosaico se muestra a través de información que debe guardar datos de la persona, teniendo que cerrar la conectividad de los datos con el ciberespacio para evitar la trazabilidad de la información (Alcala, 1998).	La investigación define que las entidades financieras mantener en un espacio protegido nuestra información, siendo posible la legitimidad de los datos que se maneja en los centros financieros.
Referencia:	Alcala, H. (1998). El Derecho a la privacidad y la intimidad en el ordenamiento juridico chileno. Chile: Universidad de Talca.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Miranda Barboza, Rodrigo	2012	Según Miranda (2012) la teoría del mosaico consiste: En no tomar un punto de vista fijo, utilizando diversas investigaciones sobre lo real. El autor creía que así era posible, a través de una colección de innumerables casos, aforismos y metáforas, realizar un proceso de yuxtaposición que permitiese un mismo mosaico de ejemplos, percibiendo así patrones y relaciones significativas entre ellos (p.148)	Se verifica que la teoría del mosaico se puede ver a través de experiencias y conocimiento, que se vuelva un proceso que proceda a jerarquizar actividades o funciones, reflejando modelos para que ocurra conexiones entre modelos (Miranda, 2012).	El proceso cuando se organiza y se jerarquiza lleva a una investigación a poder definir diferentes estrategias para estructurar un sistema que pueda llevar una solución la investigación.
Referencia:	Miranda, R. (2012). Principales acusaciones contra su obra. España: Revista Infoamerica. (Vol. 7, págs. 145-158).			

Teoría 3: Teoría de la Información				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Osear Johansen Bertoglio	1982	Según Johansen (citado por J.J. Miller, 1982) la Teoría de la información define: Señala que, mientras más complejos son los sistemas (entendiéndose por complejidad el número posible de estados que puede presentar cada parte y el número de las posibles relaciones entre esas partes) mayor es la energía que dichos sistemas destinan tanto a la obtención de la información como a su procesamiento, decisión, almacenaje y/o comunicación (p.29-30).	Por lo que se refiere la teoría que las diversas dificultades tienen en los sistemas representa el estado por la coordinación que tienen los conectores para obtener una información resguardada durante el proceso (Johansen, 1982).	La teoría permite ver que los sistemas tienen en el interno diversos complejos de rangos y mediante la operación, la información que tiene debe ser conservada durante los procesos de protección de datos que tienen la empresa.
Referencia:	Johansen, B. (1982). Introducción a la Teoría General de Sistemas. Mexico: LIMUSA Grupo Noriega Editores.			

Autor/es	Año	Cita	Parafraseo	Aplicación en su tesis
Cándido López y Manuel Veiga	2002	Según Lopez & Veiga (2002) la teoría de la información define: El nombre de entropía y constituye el pilar básico de toda la Teoría de la Información. La entropía representa el número mínimo de símbolos necesarios para codificar sin pérdida de información los estados (mensajes) de la fuente, siempre que el número de éstos sea suficientemente grande (desde un punto de vista estadístico): a menor cantidad de información, mensajes más cortos. Este es uno de los resultados centrales de la Teoría de la Información y se lo conoce habitualmente como teorema de Shannon de codificación de fuente (p.29).	En la teoría se explica que un número corto en la codificación no puede representar una pérdida de información, pero si el mensaje es grande en la fuente de datos seria expuesto a la perdida de información (Lopez y Veiga, 2002).	Explica que los mensajes cortos o largos en la fuente de datos de cualquier entidad puede originar una pérdida de información, siendo una gran amenaza para la entidad, de manera que el dato es fundamental para dar el seguimiento a un cliente.
Referencia:	López, C., & Veiga, M. (2002). Teoría de la Información y Codificación. España: Universidad de Vigo.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Jorge Uscatescu Barrón	1973	Según Uscatescu (1973) la teoría de la información es : Planteada en su perspectiva ontológica. Tema al mismo tiempo preliminar, ya que sin una clara percepción suya, los otros aspectos de la Información permanecen en una zona oscura, indefinida, condenada a un destino de permanente ambigüedad. Porque la Información es, ante todo, juego de lenguaje y silencios, de palabras dichas que encierran la muerte y revelan las paradojas dela conciencia y el despliegue de vastos medios de comunicación que no hacen sino aumentar una trágica, lunar, soledad del hombre, en el vasto hormiguero que encierra su existencia (p.5).	La teoría de la información define que es una conexión entre la información o datos semejantes, viendo que las descripciones de la información sean semejantes y no información alteradas que reflejen errores, teniendo medio para verificar que todo lo expuesto en la información es auténtico y claro (Uscatescu, 1973).	La investigación que hemos realizado para poder llegar a una solución se debe tener información, claros y precisos para poder llegar a una solución que resuelva el problema que tienen las entidades financieras.
Referencia:	Uscatescu Barron, J. (1973). Teoría de la Información. España:Revista de estudios politicos. (Vol. 192, págs. 53-74).			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**

José Luis Cuenca Tadeo	1999	Según Cuenca (1999) la teoría de la información involucra: Principalmente a una fuente de información que es codificada y transmitida desde un canal al receptor, donde se descifra. Hay dos versiones de la teoría de la información, una continua y otra discreta. La primera se preocupa de la longitud de onda, la amplitud, y la frecuencia de las comunicaciones señalizadas, y la segunda se asocia con los procesos estocásticos (azar) de la teoría automática (p.7).	Con la teoría de la información podemos encontrar códigos que pueden transmitir medios para poder tener conexión, dando al usuario medios para que acoja el mensaje enviado, siendo estas conexiones maneras de recibir comunicación e información de los procesos, siendo este medio confiable y discreto ante las conexiones (Cuenca, 1999).	La investigación lo que trata es que los colaboradores de diferentes áreas tengas maneras de tener accesos a los diferentes sistemas, en sentido optimo y confiable, ya que la información que nos otorgar ha sido guardado transparentemente.
Referencia:	Cuenca, J. (1999). "Física, teoría de la información y economía: tres lugares comunes para la entropía". España: Universidad Autonoma de Madrid.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Lopez García Candido y Fernández Veiga Manuel	2002	Según García & Fernández (2002) los resultado de la teoría de la información representa: Que la entropía representa el número mínimo de símbolos necesarios para codificar sin pérdida de información los estados (mensajes) de la fuente, siempre que el número de éstos sea suficientemente grande (desde un punto de vista estadístico): a menor cantidad de información, mensajes más cortos (p.29).	La teoría trata de explicar que la información puede ser expresada a través de datos, iconos, números, para cubrir el principal mensaje que tiene la información, siendo la expresión segura en la longitud de los datos que representa para ver el mensaje (Garcia & Fernandez, 2002).	La información que usa un usuario debe tener medios para poder proteger la información confidencial y secreta de la organización, siendo esto nuestro mayor vista para cuidar nuestro mensaje que otorga la información.
Referencia:	García, C., & Fernández, M. (2002). Teoría de la Información y Codificación. España: Universidad de Vigo.			

Teoría 4: Teoría del desarrollo organizacional				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Guizar Montufar	2013	Según Montufar (2013) la Teoría de Desarrollo Organizacional contiene: El DO se concentra en la solución de problemas, capacita a los participantes para identificar y solucionar problemas en lugar de solo analizarlos teóricamente. El DO depende en gran medida de la retroalimentación que reciban los participantes para ayudarles a sustentar sus decisiones (p.9).	En cuanto al desarrollo organizacional se manifiesta en la reparación del problema, orientando a los usuarios a identificar medidas estratégicas ante una dificultad, retroalimentando a los usuarios a capturar mejores decisiones (Montufar, 2013).	Define que para reparar el problema hay que observar y dar una solución al problema que pone en riesgo a la empresa, de manera que con la ayuda de la toma de decisiones se pueda adaptar a los diversos ataques tecnológicos y estructurales.
Referencia:	Montufar Guizar, R. (2013). Desarrollo Organizacional principio y aplicaciones. Mexico: McGRAW-HILL/INTERAMERICANA EDITORES, S.A.			

Autor/es	Año	Cita	Parafraseo	Aplicación en su tesis
Gallarzo, Espinoza & Hernandez	2011	Según Gallarzo, Espinoza & Hernandez (citado por Vaill, 2011) la Teoría de Desarrollo Organizacional contiene: El DO es "un proceso para mejorar procesos", es decir, es un proceso de la organización para comprender y mejorar cualquiera y todos los procesos justificativos que pueda desarrollar una organización para el desempeño de cualquier tarea y para el logro de cualquier objetivo.(p.8)	En la teoría el desarrollo organizacional define que la mejora de un proceso que representa a la empresa para el crecimiento de sus actividades y el éxito de sus objetivos (Gallarzo, Espinoza & Hernandez, 2011).	En definitiva, la mejora del proceso de la empresa representa el equilibrio de sus actividades para incrementar la protección que beneficiara un gran resultado en sus objetivos.
Referencia:	Gallarzo, M., Espinoza, J., & Hernandez, J. (2011). Desarrollo Organizacional. Mexico: Pearson Educacion por Mexico.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Jorge A. Hernández Palomino, Manuel Gallarzo y José de J. Espinoza Medina	2011	Según Gallarzo, Espinoza & Hernandez (citado por Kerlinger, 1979) la teoría de desarrollo organizacional es: Un conjunto de estructuras (conceptos), definiciones y proposiciones interrelacionados que presentan un punto de vista sistemático de los fenómenos, especificando las relaciones entre las variables, con el propósito de explicar y predecir los fenómenos" (p.338).	La teoría desarrollo organizacional es conformado a través de formas que define relación con diferentes campos o áreas del sistema, siendo este medio una conexión con las diversos objetivos que tiene los eventos o hechos que sucede en la organización (Gallarzo, Espinoza & Hernandez, 2011).	En la investigación nos muestra que debemos tener relación con las áreas y los proceso que tiene la financiera, ya que con la ayuda de ellos definiremos los accesos que deben tener sus compañeros.
Referencia:	Montufar Guizar, R. (2013). Desarrollo Organizacional principio y aplicaciones. Mexico: McGRAW-HILL/INTERAMERICANA EDITORES, S.A.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Manuel de Jesús Moguel Liévano	2012	Según Moguel (citado por Robert Blake y Jane Mouton, 1969), para construir la teoría de desarrollo organizacional se debe: Identificar una serie de cambios en la escena industrial, que pueden presentarse por tres vías de desarrollo: a) por evolución, b) por revolución, y c) por medio del cambio sistemático, en el cual tiene lugar la aplicación del modelo de grid para buscar la excelencia empresarial, acuñando el término al identificar una brecha entre lo que es y lo que debería ser en las organizaciones (p.57).	Se identifica que la teoría de desarrollo organizacional se realiza modificaciones ya que nos ayuda a crear; modernidad, transformación y una variación minuciosa, siendo excelentes para la norma administrativa, significando el reconocimiento de los eventos de gran riesgos o perdida que tiene la compañía (Moguel, 2012).	Siempre una nuevo desarrollo y metodología es una señal de cambio que lleva a levantar principales eventos que arriesgan nuestra sistema, o medio donde accedimos nuestra información, siendo esto un hecho primordial de la investigación.
Referencia:	Moguel, J. (2012). Aportaciones del desarrollo organizacional a la responsabilidad social de las empresas. Mexico: Universidad Autónoma de Chiapas. Administración para el desarrollo.			

Autor/es	Año	Cita	Parafraseo	Aplicación en su tesis
Robert Dailey	1990	Según Dailey (1990),para entender la teoría de desarrollo organizacional se debe: Aplicar de manera inmediata lo que está aprendiendo a los problemas que tiene que enfrentar en su trabajo. Esto le permitirá no sólo obtener una visión más amplia de esta disciplina eminentemente práctica, sino también encontrar formas de renovar su filosofía de gestión, a fin de reflejar sus nuevos conocimientos sobre el CO y aplicarlos a su trabajo (p.14).	La teoría de desarrollo organizacional señala que formarse de los problemas que ocurren en el nuestro centro laboral, es una forma de adquirir conocimiento, siendo este mecanismo la manera de alimentar nuestros fundamentos, que nos lleva a observar un novedoso entendimiento del desarrollo organizacional (Dailey. 1990).	La investigación nos lleva a captar nuevos medios para poder solucionar riesgos y problemas que tienen el área de seguridad de información de una financiera.
Referencia:	Dailey, R. (1990). Comportamiento Organizacional. Edinburgh : Escuela de Negocios de Edimburgo - Heriot-Watt University.			

Teoría 5: Teoría de Control				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Ing. Mario Alberto Perez., Ing. Analía Perez Hidalgo y Bioing. Elisa Perez Berenguer.	2008	Según Perez, Hidaldo y Berenguer (2008) explica que la teoría de control tienen: Métodos de respuesta de frecuencia y del lugar de las raíces que son el corazón de la teoría de control clásica, llevan a sistemas que son estables y que satisfacen un conjunto de requerimiento de funcionamiento más o menos arbitrarios (p.4).	La teoría de control nos permite identificar estrategias de reparo, para poder crear a los sistemas una función uniforme, que pueda enmendar el grupo de solicitudes activos o las peticiones injustificadas (Perez, Hidaldo y Berenguer, 2008)	El control nos permite poner en práctica a los sistemas las diferentes solicitudes importantes que requieren las áreas, siendo este medio un método de observar las peticiones que más necesitan.
Referencia:	Perez, M., Hidaldo, A., & Berenguer Perez, E. (2008). Introducción a los sistemas de control y modelo matemático para sistemas lineales invariantes en el tiempo. Argentina: Universidad Nacional de San Juan.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Ali Carrillo Paz	2011	Según Carrillo (2011) considera que la teoría de control esta: Basado en los objetivos que se persiguen al tratar de controlar un sistema, para que opere bajo parámetro definidos previamente. Definimos un sistema de control como el conjunto de elementos que funcionan de manera concatenada para proporcionar una salida o respuesta deseada (p.19).	Siendo la teoría de control un método de poder inspeccionar un procedimiento del sistema, para siga manejando con indicadores específicos, siendo este examen un grupo de herramientas que trabaja de manera vertical para tener un resultado o una contestación (Carrillo, 2011).	En la investigación nos muestra que los sistemas es el medio primordial, siendo los sistemas un factos para llevar a la manipulación de la información.
Referencia:	Perez, M., Hidaldo, A., & Berenguer Perez, E. (2008). Introducción a los sistemas de control y modelo matemático para sistemas lineales invariantes en el tiempo. Argentina: Universidad Nacional de San Juan.			

Autor/es	Año	Cita	Parafraseo	Aplicación en su tesis
Alfonso Tocancipa	1976	Según Tocancipa (1976) la teoría de control es: su aplicabilidad a procesos de tipo general. Entenderemos por proceso algún movimiento o acción que tenga lugar a medida que el tiempo transcurre. En general tendremos a considerar una "planta" o "sistema', cuyo estado se describe por un punto en un espacio usualmente llamado espacio de fase (p.30).	Una función conlleva a que la teoría de control tenga una etapa usual, en sus actividades siendo esto modificada por el transcurso del tiempo, que conlleva a crear estado o ciclos que pueda estar considerados en los sistemas (Tocancipa, 1976).	El proceso nos lleva con el tiempo a poder ver rediseños o cambios en los sistemas, considerando esto un medio para eliminar o atacar las nuevas amenazas, siendo que estas puedan obtener información confidencial o secreta de las entidades financieras.
Referencia:	Tocancipa, A. (Universidad Nacional de Colombia de 1976). Teoría de Control. Colombia: Repositorio institucional Universidad Nacional de Colombia.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Eduardo Cerpa	2009	Según Cerpa (2009) considera que la teoría de control analiza: las propiedades de este tipo de sistemas. Por ejemplo, la pregunta básica que podemos estudiar es la factibilidad de llevar un sistema desde un estado inicial a un estado final en un tiempo dado. Además, podemos considerar ciertos criterios o restricciones para la función de control o el estado (p.2).	Analizar la teoría de control conlleva a verificar las variedades de sistemas, siendo esto una forma de conocer que el sistema desde su etapa original, a su ciclo definitivo, se ha definido pautas o trabas para llevar a un buen estado de control de este (Cerpa, 2009).	En el estudio nos presenta que para poder acceder a los sistemas debemos tener definidos los perfiles para poder manejar la información, teniendo que ver que los sistemas tengan claros los perfiles que tienen los colaboradores.
Referencia:	Cerpa, E. (2009). Introducción a la Teoría de Contro. Venezuela: Universidad Santa María.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Carlos A. Smith y Armando B. Corripio	1991	Según Smith y Corripio (1991) la teoría de control se: Utilizan casi exclusivamente estas variables y, por tanto, se debe comprender bien el significado e importancia de las variables de desviación. Como se explicó en el capítulo 2, con su uso se tiene la ventaja de que su valor indica el grado de desviación respecto a algún valor de operación de estado estacionario; en la práctica, este valor de estado estacionario puede ser el valor deseado :de la variable (p.94).	En la teoría de control maneja variante que conlleva a analizar el concepto que tienen las variantes, teniendo el beneficio de que el costo pueda tener un cambio extraordinario, pero vemos que el costo puede representar una variante deseado (Smith y Corripio, 1991)	En nuestro estudio tener control de los sistemas que maneja los colaboradores conlleva que los perfiles que tienen los usuarios es el valor que permite acceder a diversos documentos que fomentan la comunicación de la información obtenida.
Referencia:	Smith, C., & Corripio, A. (1991). Control Automático de Procesos. Mexico: EDITORIAL LIMUSA.			

5. Matriz de antecedentes

Datos del antecedente internacional: 1		Redacción final
Título	*Metodología para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 2700*	Según Valencia y Orozco (2017) en el artículo nominado *Metodología para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 2700*, cuyo objetivo es plantear un sistemas de gestión de seguridad de información explicando los principales bases de las normas iso, dando la comparación entre seguridad de información y seguridad informática, aportando a la organización un motivo decisivo en la SGSI. Al final del artículo, se concluyó que las alternativas para establecer un buen accionamiento en la gestión de seguridad de información que se entabla por procesos complejos para el establecimiento de un proceso metodológico, otorgándole una interrelación que existe con las diversas normas de la iso, para encaminar con los estándares que existen a la organización, siendo este medio para abordar proyectos que precisen los profesionales.
Autor	Valencia y Orozco	
Año	2015	
Objetivo	Es plantear un sistema de gestión de seguridad de información explicando las principales bases de las normas iso, dando la comparación entre seguridad de información y seguridad informática, aportando a la organización un motivo decisivo en la SGSI.	
Metodología		
Tipo		
Enfoque		
Diseño		
Método		
Población		
Muestra		
Técnicas		
Instrumentos		
Método de análisis de datos		
Resultados		
Conclusiones	Las alternativas para el establecimiento de una autoridad de control en materia de protección de datos personales son varias. La primera, es la creación de una agencia autónoma constitucional, similar al CPLT, exclusivamente dedicada a la protección de datos personales; la segunda, es otorgarle al CPLT esa atribución; la tercera, encomendarle esa función a otros órganos del Estado, como el Sernac, alguna superintendencia o, incluso, dispersar sus competencias entre distintos órganos públicos. - La injerencia del CPLT en materia de tratamiento de datos personales es indirecta, pues solo proporciona directrices en orden a limitar la intervención estatal -cuando es un órgano de la administración del Estado el que realiza el tratamiento de datos personales- o cuando debe resolver reclamaciones en solicitudes de acceso a información pública que contenga datos personales, conforme a la normativa legal, sin tomar un rol activo en la defensa y promoción del resguardo de los mismos.	
Referencia	Valencia Duque, F., & Orozco Alzate, M. (2015). Metodología para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 2700. Colombia: Revista Ibérica de Sistemas y Tecnologias de Información. (Vol. 22, págs. 73-88)	

Datos del antecedente internacional: 2		Redacción final
Título	*Desarrollo de un modelos de seguridad para la prevención de pérdida de datos dlp, en empresas pymes.*	Según Acosta (2015) su investigación denominado *Desarrollo de un modelo de seguridad para la prevención de pérdida de datos dlp, en empresas pymes*, con el objetivo es definir un boceto de seguridad de información para llevar a cabo la custodia de los datos en las pequeñas y medianas empresa, siendo una herramienta que prevé el extravió de la información sociedades pymes. En la investigación se describe la metodología descriptiva debido a que incluye un estudio inductiva, deductiva y experimental, se llevó a cabo el sistema DLP endpoint en la organización. Con la ayuda de la metodología deductiva se podrá validar y reconocer los eventos problemáticos que está ejecutando en la empresa actualmente. La investigación les permitió concluir, que el extravió de información de la organización puede generar un daño en la información que tiene la empresa, se explicó dos obstáculos: el fallo tecnológico y la dificulta humana. Se infiere que la ejecución del boceto para la custodia de los datos a sido satisfactorio, ya que se podido disminuir los conceptos tecnológicos que opera en tiempo real la información de la empresa.
Autor	Ximena Acosta Robles	
Año	2015	
Objetivo	Proponer un modelo de seguridad para la implementación que esta directamente relacionada con la prevención de perdida de datos en las empresas pymes	
Metodología		
Tipo	Carácter Descriptivo	
Enfoque	Inductiva, Deductiva y experimental	
Diseño		
Método		
Población		
Muestra		
Técnicas		
Instrumentos		
Método de análisis de datos		
Resultados		
Conclusiones	La investigación les permitió concluir, que las posibles causas puede generar la pérdida de información en las empresas pymes del Ecuador, definiendo dos elementos principales para este problema: el tecnológico y el humano. Se infiere que el desarrollo del modelo de prevención de pérdida de datos se logró mitigar favorablemente en el aspecto tecnológico tener una herramienta que gestione todo el seguimiento de la información clasificada en tiempo real y en el aspecto humano tener el suficiente conocimiento de lo que implica el perder la información.	
Referencia	Acosta, X. (2015). Desarrollo de un modelos de seguridad para la prevención de pérdida de datos dlp, en empresas pymes. Quito.	

Datos del antecedente internacional: 3		Redacción final
Título	*Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado*	Según Sanz (2015) en el artículo nombrado Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado. El articulo definió como objetivo, que el estado deben publiquen de
Autor	Francisco Javier Sanz Salguero	
Año	2015	
Objetivo	i) que las entidades del Estado divulguen de manera permanente información sin mediar	

		requerimiento expreso de un ciudadano ("mostrar"), situación que se enmarca dentro de la transparencia activa, y ii) que las entidades del Estado, en relación con aquella información en su poder que la ley no obliga a publicar activamente, entreguen los datos que sean requeridos por cualquier ciudadano (siempre que no corresponda a información de carácter secreto o reservado), situación que se enmarca dentro del "derecho de acceso a la información pública" propiamente dicho (lo que involucra un "permitir ver" o derecho de "saber"). En consecuencia, el acceso a la información pública se identifica como un mecanismo central en favor del logro de la transparencia en lo público.	manera indefinida información sin controlar las peticiones de los usuarios, como la opción de mostrar, esta realidad se centra en la claridad activa, y por último se tomó como objetivo que los organismos públicos, en unión con la información está en su poder que el reglamento no obliga al publicar, otorgar datos que sean de gran importancia por el ciudadano (teniendo en claro que no debe ser usada la información privada del usuario), la realidad es que el derecho a obtener acceso a dicha información pública, que según se define en otorgarles derechos o permitir y saber. En consecuencia, cuando se obtiene acceso a la información de otro usuario se verifica técnicas para lograr una mejor transparencia en usuario común. Al final, se determinó que el acceso a la información privada de un usuario común es un derecho que debe tener el individuo y cualquier otra persona, para investigar u obtener los datos que necesitamos (con independencia constancia y control de los expedientes) en poder de cualquier ente o persona pública, de cualquier sociedad, grupo o corporación privado o independiente de la propiedad del estado o siendo controlado por él, y de alguna cooperativa particular (con el trato de que la empresa reciba apoyo común o que tengan labores y funciones cotidianas, pero solo con respecto a las bases o asistencia públicos realizado, para el buen funcionamiento de nuestro país y de los datos que dan un persona común ante la sociedad), la conexión deber ser bloqueado por privilegios taxativas que respecten el reglamentos de una colectividad demócrata.
Metodología			
	Tipo	Cualitativo	
	Enfoque		
	Diseño		
	Método		
	Población		
	Muestra		
	Técnicas		
	Instrumentos	Identificar dos tipos de instrumentos: en primer lugar tenemos el principio de la "transparencia máxima", al que Toby Mendel26 le ha otorgado el carácter de "principio clave que fundamenta" el acceso a la información y, en segundo lugar, tenemos lo que hemos denominado como principios orientadores. A continuación, realizaremos el trabajo enunciado.	
	Método de análisis de datos		
Resultados			
Conclusiones		Definimos el derecho de acceso a la información pública como el derecho humano fundamental que tiene cualquier persona, para buscar o recibir cualquier tipo de dato (con independencia del formato o medio de control y archivo) en poder de cualquier autoridad pública, de cualquier órgano, organismo o entidad independiente o autónomo de propiedad del Gobierno o controlado por el mismo, y de cualquier organización privada (siempre y cuando, en este último caso, que la organización reciba fondos o beneficios públicos sustanciales o que desempeñan funciones y servicios públicos, pero solamente con respecto a los fondos o beneficios públicos recibidos o a las funciones y servicios públicos desempeñados), acceso restringido solo por las excepciones taxativas que establezca la ley en una sociedad democrática.	
Referencia		Sanz Salguero, F. (2015). Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del	

	derecho comparado. Colombia: Revista Ius et Praxis. (Vol. 22, págs. 323-376).

Datos del antecedente internacional: 4		Redacción final
Título	*Conceptos y legislación de transparencia sindical y protección de datos personales de los trabajadores en México*	Según Aparicio (2017) el articulo denominado Conceptos y legislación de transparencia sindical y protección de datos personales de los trabajadores en México, el objetivo del artículo es obtener un eficaz y eficiente ejercicio para las actividades de las organizaciones, y evaluar que estos objetivos se cumpla según su creación, es decir: la investigación, mejoramiento y la protección del grupo del sindicato. El trabajo de estudio se concluyó que la espera que tiene la transparencia sindical sirva como un medio de instrumento que ejercer los derechos de los obreros, como los principales actores que ejercen una función importante en el área laboral siendo su deber obtener un negociación social, para llevar a cabo se debe respetar sus derechos laborales; y no sea una herramienta para dificultar la claridad, siendo un modo de sanción a las agremiados exteriores que tienen intereses organizacionales, eliminando los pocos grupo sindicales independiente. Sin embargo, el tema de reguardo de los datos de los trabajadores es el principal situación, así como el trato que otorga la empresa a los trabajadores. Por consiguiente, las nombradas "listas negras" se muestran como una alerta del mal funcionamiento que se tiene en el uso de los datos de los trabajadores, para restringir la comunicación de los empleados a sus compañeros de trabajo. De manera que, los propios sindicatos tienen la obligación de mantener una clara información sindical, sino también en el cuidado de sus datos que tienen en a su custodia, y como se ha visto en la investigación, muy poco se ha comentado sobre este tema.
Autor	Aparicio Velázquez	
Año	2017	
Objetivo	lograr un eficaz y eficiente ejercicio del quehacer de estas organizaciones, y verificar que se cumpla con el objetivo de su creación, es decir: el estudio, mejoramiento y defensa de los derechos de los agremiados. Con esta definición debe distinguirse la exógena y la endógena como antes se explica.	
Metodología	Exploratoria	
Tipo	Cualitativo	
Enfoque		
Diseño		
Método	Régimen de tutela de los datos personales asociado al ejercicio del derecho de acceso a la información pública en el derecho comparado	
Población		
Muestra		
Técnicas		
Instrumentos		
Método de análisis de datos		
Resultados		
Conclusiones		
Referencia	Aparicio, J. (2017). Conceptos y legislación de transparencia sindical y protección de datos personales de los trabajadores en México. Mexico: Universidad Nacional Autònoma de Mexico.	

Datos del antecedente internacional: 5		Redacción final
Título	*La Protección de Datos de Carácter Personal en los Contratos Electrónicos con Consumidores: Análisis de la Legislación Colombiana y de los Principales Referentes Europeos*	Según Monsalve (2016) el artículo nominado *La Protección de Datos de Carácter Personal en los Contratos Electrónicos con Consumidores: Análisis de la Legislación Colombiana y de los Principales Referentes Europeos*, el objetivo que definió el artículo es examinar el contexto que regula el estado colombiano que se aplica a los eventos de los datos confidenciales de los consumidores que son ingresado por un usuario al sistema que se manifiesta en un contrato electrónico, siendo como conocimiento a los directivos que están al máximo rango de la legislación europea. Al final del estudio el reglamento de los datos personales que tiene como propósito resguardar la información de los consumidores y la sociedad viene a fortalecer los registros digitales y/o electrónicos el compromiso de otorgar a la información precontractual y pos-contractual que ha sido debilitado por los proveedores o expendedores, al ser impuestos a manifestar la determinación del proceso de datos personales obtenidos por el manejo de los contrato, con miras a establecer una aprobación y permiso independiente, definido o comunicado por los clientes y proporcionar autenticidad y claridad en el momento del recaudo e gestión de la investigación de los datos privados de los clientes.
Autor	Monsalve Caballero	
Año	2016	
Objetivo	El objeto el análisis del marco regulatorio colombiano 1 aplicable a los casos en que los datos personales son incorporados por un consumidor a la red con ocasión de un contrato electrónico, teniendo como referente las principales directivas y legislación europea de mayor relevancia en la materia	
Metodología		
Tipo	Cualitativa	
Enfoque		
Diseño		
Método		
Población		
Muestra		
Técnicas		
Instrumentos		
Método de análisis de datos		
Resultados		
Conclusiones	La LPDP viene a reforzar en los contratos electrónicos las obligaciones de información precontractual y pos contractual que recaen sobre los proveedores o expendedores, al ser obligados a declarar la finalidad del tratamiento de datos personales recaudados con ocasión del contrato, con miras a asegurar el otorgamiento de un consentimiento libre, específico e informado por parte de los consumidores y adotar de legitimidad y transparencia el recaudo y administración de la base de datos.	
Referencia	Monsalve Caballero, V. (2016). La Protección de Datos de Carácter Personal en los Contratos Electrónicos con Consumidores: Análisis de la Legislación Colombiana y de los Principales Referentes Europeos. Mexico: Revista Prolegómenos. (Vol. 1, págs. 163-195).	

Datos del antecedente internacional: 1		Redacción final
Título	*Implementación de un sistema de Gestión de la Seguridad de la Información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001*	Según Tola (2015) la investigación denominada *Implementación de un sistema de Gestión de la Seguridad de la Información para una empresa de*
Autor	Diana Elizabeth Tola Franco	

Año	2015	*consultoría y auditoria, aplicando la norma ISO/IEC 27001*, cuyo objetivo de la investigación es promulgar un sistema de gestión de seguridad de la información para defender la reserva, integridad y existencias de los testimonios de la empresa A&CGroup S.A., la metodología que se refleja en la investigación en sobre el PDCA (Plan-Do-Check-Act) y la metodología MAGERIT en la que considera un tácticas sistemáticos que permita examinar los eventos, iniciando medios para un buen resultado. La investigación llevo a la conclusión, que cuando hallamos sucesos inseguros coloca a los activos de información a una exhibición causando pérdidas siendo imprescindible asignar controles, con el fin de custodiar los activos de información. También, es significativo fijar régimen y directrices que encaminen a la organización a propiciar su información.
Objetivo	es promulgar un sistema de gestión de seguridad de la información para defender la reserva, integridad y existencias de los testimonios de la empresa A&CGroup S.A.	
Metodología		
Tipo	sobre el PDCA (Plan-Do-Check-Act) y la metodología MAGERIT en la que considera un tácticas sistemáticos que permita examinar los eventos, iniciando medios para un buen resultado.	
Enfoque		
Diseño		
Método		
Población		
Muestra		
Técnicas		
Instrumentos		
Método de análisis de datos		
Resultados		
Conclusiones	que cuando hallamos sucesos inseguros coloca a los activos de información a una exhibición causando pérdidas siendo imprescindible asignar controles, con el fin de custodiar los activos de información. También, es significativo fijar régimen y directrices que encaminen a la organización a propiciar su información.	
Referencia	Tola Franco, D. (2015). Implementación de un sistema de Gestión de la Seguridad de la Información para una empresa de consultoría y auditoria, aplicando la norma ISO/IEC 27001. Ecuador: REPOSITORIO DE ESPOL.	

Datos del antecedente Nacional: 1		**Redacción final**
Título	*La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales*	Según Alvarado (2016) el articulo denominado La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales, siendo el propósito de favorecer un inserción de un proceso de evaluación continua, por medio de la clasificación de los conjunto de datos de los clientes que tienen la empresa en comprensión a los riesgos que se está midiendo la susceptibilidad y método dado a esta investigación, que se añade a los procesos técnicos, orientar a los usuarios naturales que usen en su ambiente laboral y profesional una protección, y
Autor	Francisco Javier Alvarado	
Año	2016	
Objetivo	Es facilitarla implantación de una gestión en continua evaluación que, mediante la categorización de los bancos de datos personales en razón a los riesgos que conlleva su sensibilidad y el tratamiento dado, complemente las medidas técnicas; Informar a los usuarios para que tomen conciencia de la protección requerida; y exigir un nivel de seguridad equilibrado entre los riesgos, las técnicas de seguridad y el costo de las medidas.	
Metodología	muchas de las reglas propias de grupos profesionales son documentadas actualmente	

	en forma de códigos, normas técnicas o protocolos de actuación que hacen más fácil las relaciones entre el ámbito profesional y el jurídico	solicitar un grado de seguridad que provee los riesgos, los métodos de seguridad y el precio de los métodos que se está incorporando a esta medida. En este artículo está orientada a una metodología que sigue diversos principios propios a equipos de gran alta de profesionalismo que hoy en día son archivados en forma de códigos, políticas o actas de eventos que hacen más común la asociación entre el ambiente profesional y legal. Como resultado obtenidos en la investigación, se obtuvo que seguir ciertos dominios de defensa ante los peligros de ataque que no se obtiene hoy en día como resultado de un método que va observando las debilidades y peligros latentes que van causando ciertos eventos de deterioro o destrucción en el ambiente. En definitiva se concluyó, que la gestión de evaluación continua va distinguir las debilidades y señal de peligros, motivos y la posibilidad de que vuelva a suceder y el agravia que provocaría .En definitiva incorporar ciertos dimensiones de seguridad es determinada por el incremento de registros y ubicuidad del conjunto de datos que tiene la empresa, el valor y el manejo de los datos por cada individuo, el periodo de su procedimiento y el compromiso del titular del conjunto de datos.
Tipo	Cualitativo	
Enfoque		
Diseño		
Método		
Población		
Muestra		
Técnicas		
Instrumentos		
Método de análisis de datos		
Resultados		
Conclusiones	La implementación de determinadas medidas de seguridad es requerida, según corresponda, a categorías establecidas en relación con el volumen de registros y ubicuidad del banco de datos, el número y calidad de datos por persona, el plazo para su tratamiento y la calidad del titular del banco de datos.	
Referencia	Alvarado, F. (2016). La gestión de la Seguridad de la Información en el régimen. Lima: Revista Foro Jurídico. (Vol. 15, págs. 26-41).	

Datos del antecedente Nacional: 2		**Redacción final**
Título	*El derecho a la protección de Datos Personales Algunos temas relevantes de su regulación en el Perú*	Según Eguiguren (2015) en el artículo bajo el titulo *El derecho a la protección de Datos Personales Algunos temas relevantes de su regulación en el Perú*, cuyo objetivo de la ley de los derechos de los datos personales es aplicar que toda información, inscripción, formato, expedientes, conjunto de datos personales que sea ha establecido como una tarea financiera, científica, de estudio entre otros; definida al puesto de la sociedad pública o privada., puede ser protegida si tiene como titula a una persona natural
Autor	Francisco José Eguiguren Praeli	
Año	2015	
Objetivo	la regla general es que la LPDP será de aplicación a todos los archivos, registros, bancos o bases de datos personales que se establezcan en cualquier tipo de actividad económica, laboral, administrativa, científica, etcétera; sea que estén a cargo de entidades privadas o públicas, salvo que tengan como titular a personas naturales –para su uso privado– o a entidades públicas, únicamente cuando estén relacionados o sean necesarios para el cumplimiento de sus competencias institucionales, en materias como	

	defensa nacional, seguridad pública, y acción penal de investigación y represión del delito.	para el manejo de la sociedad privada o pública, siendo este medio para la asignación de las capacidades organizacionales, en función a defensa nacional, protección pública y medida penal para el estudio y sometimiento del delito. Al final es estudio permitió que se reconozca y se sugiera constitucionalmente una optimización a los derechos confidenciales que tiene cada persona en su vida privada, siendo este flujo como un medio de crecimiento a las nuevas innovaciones que tiene la era tecnológica de la información. El cuidado y medición es evento primordial para otorgar al titular o al cliente el derecho de tener el máximo fase de control y decisión autónoma sobre la información privada y datos a su persona.
Metodología		
Tipo	Cualitativo	
Enfoque		
Diseño		
Método		
Población		
Muestra		
Técnicas		
Instrumentos		
Método de análisis de datos		
Resultados		
Conclusiones	Su surgimiento y reconocimiento constitucional supuso una automatización del derecho a la intimidad personal, fuertemente influenciado por el desarrollo vertiginoso de las nuevas tecnologías de la información. Su protección y regulación se hace muy importante para garantizar que el titular de este derecho pueda tener mayor nivel de control y determinación autónoma sobre los datos personales e información referida a su persona, que se registran, sistematizan y transmiten, muchas veces sin su conocimiento.	
Referencia (tesis)	Eguiguren, P. (2015). El derecho a la protección de Datos Personales Algunos temas relevantes de su regulación en el Perú. Lima, Peru: Revista Universidad Pontifice Católica del Perú.(Vol. 67, págs. 131-140).	

Datos del antecedente Nacional: 3		**Redacción final**
Título	*No se lo Digas a nadie, pero tengo un banco de Datos de Clientes Sensibles, La Gestión de la Protección de Datos de Personales en el Sistemas Financiero para la Prevención de Lavado de Activos*	Según Haza (2015) en el artículo denominada No se lo Digas a nadie, pero tengo un banco de Datos de Clientes Sensibles, La Gestión de la Protección de Datos de Personales en el Sistemas Financiero para la Prevención de Lavado de Activos., en el objetivo del artículo es mostrar que no está dispuesto ejecutar la Ley de Protección de Datos Personales que toma referencia a los usuarios débiles y al público que denominado PEP, llamados usuarios que son expuesto públicamente en el contenido de la
Autor	Antonio de la Haza Barrantes	
Año	2015	
Objetivo	Nuestro objetivo a lo largo de las líneas siguientes es el demostrar que no es susceptible de aplicación la Ley de Protección de Datos Personales N° 29733 en relación a los clientes sensibles y, dentro de todos los clientes sensibles, en especial en el denominado cliente PEP en el tema de la prevención de lavado de activos.	
Metodología		
Tipo	Cualitativo	

	Enfoque	
	Diseño	
	Método	
	Población	
	Muestra	
	Técnicas	
	Instrumentos	
	Método de análisis de datos	
Resultados		
Conclusiones	Brindar una protección absoluta a la privacidad de una persona natural es partir de un paradigma equivocado, es asumir que todas las personas requieren de la protección de una autoridad nacional que se encargará de cuidar la privacidad de las personas más allá de sus decisiones, es buscar brindar protección sobre aquella información que se entiende como pública pero que la autoridad entiende que no siempre es así.	
Referencia	Haza, A. (2015). No se lo Digas a nadie, pero tengo un banco de Datos de Clientes Sensibles, La Gestión de la Protección de Datos de Personales en el Sistemas Financiero para la Prevención de Lavado de Activos. Lima, Peru: Revista de Actualidad Mercanti, Universidad Pontifice Católica del Perú. (Vol. 4, págs. 74-93).	

precaución de blanqueo de dinero. De manera, en el artículo se manipulo la metodología de innovadores paradigmas que lo podemos encontrar a través de la creación de metodologías que hallen y evalúen los riesgos, así también el resguardo de los documentos confidenciales de los usuarios que está definido en las normas de los clientes que tiene definido la organización. La sugerencia que se define en el artículo es exponer un ensayo que explique las recientes paradigmas que puntualice el reguardo de los datos de los clientes, claridad y valides en el proceso de la información y la unión que tiene los expedientes de los clientes con la gestión de riesgos. Se pudo concluir en el artículo que al otorgar custodia a los expedientes de los clientes es fundamental el secreto de la información de una cliente natural, que puede ser a partir de un paradigma erróneo, la responsabilidad de encargase de que todos los clientes sean beneficiados de tener un buen resguardo que requiera la protección de un órgano nacional que se responsabilice de mantener el cuidado de su privacidad de las personas más allá de la autoridad que tenga en el estado, dedicar una buen custodio para la información se puede entender que la información pública para el estado no siempre va ser para el manejo y uso de su poder.

Datos del antecedente Nacional: 4	
Título	*Diseño de un Sistema de Gestión de Seguridad de Información para servicios Postales del Perú S.A*
Autor	David Arturo Aguirre Mollehuanca
Año	2014
Objetivo	Diseñar un sistema de gestión de seguridad de información para SERPOST según lo indicado por la NTP ISO/IEC 27001:2008 y la NTP-ISO/IEC 17999:2007 de seguridad de información

Redacción final

Según Aguirre (2014) el trabajo denominado Diseño de un Sistema de Gestión de Seguridad de Información para servicios Postales del Perú S.A., la investigación tuvo por objetivo proyectar un sistema de administración de defensa al aclarar para SERPOST según lo indicado por la ISO/IEC 27001:2008 y la NTP-ISO/IEC 17999:2007 de

Metodología	los requerimientos para desarrollar un sistema de gestión de seguridad de la información basándose en el ciclo de DEMING, o ciclo Plan – Do – Check -Act, una metodología cíclica muy usada en las normas ISO relacionadas a normas de gestión [NTP ISO/IEC 27001].	seguridad de información. En la metodología que resalta la investigación es brindar la asistencia de las peticiones para establecer una organización de administración de defensa a la información, se utilizó el ciclo de DEMING, o también llamado circulo PDCA, Plan – Do – Check - Act, durante el estudio se manejó una metodología cíclica, que es siempre utilizada por la Organización Internacional de Normalización relacionada siempre con los reglamentos de las diferentes gestiones que la organización administra. Sin embargo, se visualizó una gran ayuda del comité debido que si el mando del grupo no se podría llevar a cabo el funcionamiento de las decisiones del equipo de trabajo, bajo los métodos, procesos y procedimientos de las normas de defensa de la empresa, ya que explica que controles se puede ejecutar durante un riesgo o amenaza, los talleres o difusiones son un medio de culturización a los colaboradores, siendo su función de manejar las normas dentro de sus área laboral, para llevar a cabo la incorporación de SGSI en nuestra empresa, se tiene que realizar los debidos normas internacionales a defensa a la información de los colaboradores, el punto que se pronuncia es una herramienta de buena práctica, ya que podemos asegurarnos que el uso y el manejo va ser eficiente en las distintas de áreas de la empresa. Al finalizar el estudio concluyo, que para implementar es de buen uso orientar los métodos y procedimientos de seguridad y defensa que están ahora en el mundo empresarial, debido al poco conocimiento que tiene los colaboradores para ejecutarlo en su empresa.
Tipo	Cualitativo	
Enfoque		
Diseño		
Método		
Población		
Muestra		
Técnicas		
Instrumentos		
Método de análisis de datos		
Resultados		
Conclusiones	Es necesario difundir las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, esto debido a la poca cultura de seguridad que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas.	
Referencia	Aguirre, D. (2014). Diseño de un Sistema de Gestión de Seguridad de Información para servicios Postales del Perú S.A. Lima: Universidad Pontifice Católica del Perú.	

Datos del antecedente nacional: 5		Redacción final
Título	*Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.*	Según Espinoza (2013) en estudio nominado Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo, en el estudio se definió como objetivo examinar y trazar una técnica de proceso de seguridad de información, apoyado por organización de estandarización ISO/IEC 27001:2005, para llevar a cabo a una organización dedicado a la fabricación y negociación. La metodología que se usó en la investigación es nombrada MAGERIT II es un método para organizar y encontrar amenazas que pueden ser las principales amenazas que vulneren y debiliten a nuestra organización, el gran aporte que nos va dar este método es que nuestra área podrá examinar las vulnerabilidades y podrá levantar las medidas, para mantener bajo fiscalización nuestros estado de riesgo. Nuestro estudio ha concluido que la técnica de proceso de seguridad a favor de la defensa de la información se organiza a los controles que tiene la gestión de fabricación y negociación que tiene actualmente la empresa, se debe coordinar con el responsables o usuarios de los procesos que fueron evaluado para la técnica de defensa al cuidado de la información de este investigación, la seguridad tiene que ser un tema de mayor interés para darle mayor importancia a la seguridad de la información, y para levantar las amenazas que pueden ser un peligro a la información que usamos diariamente en la empresa, de esta manera se debería coordinar de tomar planes de acciones sobre posibles amenazas..
Autor	Hans Ryan Espinoza Aguinaga	
Año	2013	
Objetivo		
Metodología	Magerit II	
Tipo		
Enfoque		
Diseño		
Método		
Población		
Muestra		
Técnicas		
Instrumentos		
Método de análisis de datos		
Resultados		
Conclusiones	Debe tenerse en cuenta que el diseño de SGSI presentado se adapta a los objetivos actuales del proceso de producción, en el cual se ha basado el proyecto, y que este diseño podría variar ya que los objetivos estratégicos y de gobierno de le empresa pueden cambiar y por ello algunos sub procesos que forman parte del alcance del proyecto, también lo harán. Del mismo modo, se debe establecer que los dueños de cada uno de los procesos que fueron analizados para el diseño del SGSI de este proyecto, empiecen a darle mayor importancia a la seguridad de la información, y que velen para que de alguna manera se pueda levantar los riesgos encontrados dentro de sus actividades ya que no es seguro que este diseño se logre implementar, y por ello debería ser labor de ellos el tratar de eliminar dichos riesgos.	
Referencia	Espinoza, H. (2013). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. Lima: Repositorio Universidad Pontifice Católica del Perú.	

Datos del antecedente internacional: 6		Redacción final
Título	*Implementación de un sistema de control de acceso para mejorar la seguridad de información de la empresa SNX S.A.C*	Según Rivas (2016) su estudio nominado *Implementación de un sistema de control de acceso para mejorar la seguridad de información de la empresa SNX S.A.C.*, el objetivo del estudio es imponer un sistema de control de acceso para perfeccionar la seguridad de información de la organización, afianzando una estabilidad en su información a los involucrados de la organización. El estudio concluyo que la conformación de una muestra de los accesos cuando se incorpora por roles es laborioso, pero puede ser explicados por los atenciones que solicitan los usuarios.
Autor	Miguel Alejandro Martín Rivas Arellano	
Año	2016	
Objetivo	Es imponer un sistema de control de acceso para perfeccionar la seguridad de información de la organización, afianzando una estabilidad en su información a los involucrados de la organización.	
Metodología		
Tipo		
Enfoque		
Diseño		
Método		
Población		
Muestra		
Técnicas		
Instrumentos		
Método de análisis de datos		
Resultados		
Conclusiones	la conformación de una muestra de los accesos cuando se incorpora por roles es laborioso, pero puede ser explicados por los atenciones que solicitan los usuarios.	
Referencia	Rivas Arellano, M. (2016). Implementación de un sistema de control de acceso para mejorar la seguridad de información de la empresa SNX S.A.C. Lima: Repositorio Nacional Mayor de San Marcos.	

6. Marco conceptual

Categoría: Gestión de control de accesos				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Carazo Torres Omar	2013	Según Carazo(2013) indica que la gestión de control de acceso: Los accesos son controlados mediante los privilegios de accesos a la información, donde se controla que cada empleado únicamente pueda acceder a los recursos que le están destinados para su puesto de trabajo, sin revisar, en ningún periodo de tiempo, si cada usuario tiene los privilegios que le tocan para su puesto. Sin embargo, no está documentado y accesible para los empleados a modo de que sepan la política de la compañía. Tampoco está documentado y, por donde tampoco se aplica, una política de contraseñas robusta para acceder a los servicios de información.(p.18)	La teoría de gestión de control de accesos explica que los accesos son monitoreados a través exenciones especiales para conectarse con la información que va usar, llevando un grado de inspección en las opciones del perfil según al cargo que tiene el colaborador. De manera que, si conocen el manual de procedimiento y procesos de las áreas responsables, podrán usar responsablemente la información (Carazo, 2013).	La investigación se basa en la verificación y monitoreo de los accesos que se le otorga a un colaborador, con ciertas restricciones, encargando a un responsable que tenga un control en los sistemas de la financiera.
Referencia:	Carazo, O. (2013). Elaboración de un Plan de Seguridad de la Información. España: Universidad Oberta de Catalunya.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Arantxa Mora Perez	2016	Según Mora (2013) indica que la gestión de control de acceso: Un control de accesos es un sistema electrónico que restringe o permite el acceso de un usuario o grupo de usuarios a un área específica validando la identificación por medio de diferentes tipos de lectura (clave por teclado, lector de tarjetas, biometría, etc.) y a su vez controlando el recurso (puerta, armario, torniquete, etc.) por medio de un dispositivo eléctrico como un electroimán, pestillo o motor. Un control de accesos requiere flexibilidad para que no haya limitaciones en la movilidad por cambios que se producen en los permisos. Necesita precisión para que se le asigne el permiso correcto a cada persona. Y también es necesario que tenga suficiente capacidad para almacenamiento y registro de un mínimo de datos.(p.13)	El sistema electrónico se define como una gestión de control de accesos, ya que bloquea y concede vías de conexión al usuario a las fuentes de información, dando ciertas validaciones para verificar que es el usuario indicado, la validación se realiza por diversas fuentes de lectura (lector de tarjetas, huella digital, etc.) y tiene un monitoreo que inspecciona las herramientas por medio de un programa. Para otorgar autorizaciones correctos es necesario de requerimientos específicos (Mora, 2016).	Por medio del control de accesos se otorga a los colaboradores ciertas medidas de restricciones y les concedes accesos a los informaciones que van a manejar para determinados funciones que cumple según su cargo, dando herramientas para que pueda acceder con seguridad con las diversos maquinas, programas y aplicaciones de seguridad.

Referencia:	Mora Perez, A. (2016). Gestión de Prevención. Control de acceso. España: Repositorio Universidad Policitenica de Cartagena.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
José A. Montoya S. y Zuleima Restrepo R.	2012	Según Montoya y Restrejo (2012) la gestión de control de accesos consiste: es un término que se puede entender como el conjunto de procesos de negocio, tecnologías, infraestructura y políticas que permite realizar la gestión de las identidades de usuario y controlar el acceso de éstas a los diferentes recursos organizacionales (p.25).	La gestión de control de accesos en palabra deduce como se compone los procedimientos de intereses científicos, arquitectónicos y gubernamentales que efectúa la misión de diligencia de la analogía del usufructuario y contrastar el acercamiento de los distintos tácticas de la entidades (Montoya y Restrejo, 2012).	El flujo que abarca el desarrollo del control de acceso es el panorama de los modelos que representa la conexión de los beneficiarios hacia los distintos portales que puedan alcanzar.
Referencia:	Montoya, J., & Restrepo, Z. (2012). Gestión de identidades y control de acceso desde una perspectiva organizacional. Colombia: Revista Ingenierias USBMed. (Vol. 3, págs. 23-34).			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
José Carlos Dextre Flores y Raúl Sergio Del Pozo Rivas	2012	Según Dextre y Del Pozo (2012) gestión de control de accesos se: corresponde analizar cómo se gestiona el control a través de la adopción de una estructura basada en la organización de la entidad para enfrentar con éxito los riesgos del negocio (p.74).	Coincidir con el estudio a modo de dirigir la inspección a través de acoger una forma para probar que la constitución caracteriza encarar con notoriedad la contingencia del comercio (Dextre y Del Pozo, 2012).	El estudio que efectuamos contrarresta observa de modo muy minucioso, alcanzar un ejemplo, que nos avale el dominio que tiene los eventos de perdida en el negocio.
Referencia:	Dextre, J., & Pozo, R. (2012). Administracion. En Control de gestión o gestión de control? . Lima, Peru: Revista Redalyc.(Vol. 7, págs. 69-80)			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Willman Cedeño Chavez y Salvador Muñoz Gutierrez	2000	Según Cedeño y Muñoz (2000) la gestión de control de accesos se: organice y haga congruentes los intereses de cada departamento mediante la definición de desempeños para que cada área tenga en cuenta, tanto el logro de sus propios resultados, como la contribución que estos hacen a los resultados de la empresa (p.90).	Establecer un sensato disposición de los sectores a través de sus cumplimientos, orientando este medio para cada campo consintiéndole información de sus éxitos y aportación concerniente al cometido de su acción en la firma (Cedeño y Muñoz, 2000).	El crecimiento que tienen las áreas de cada departamento es el medio para poder involucrar esquemas o propuestas a los colaboradores de enriquecer sus funciones.
Referencia:	Cedeño, W., & Muñoz, S. (2000). Control de gestión y Gestión tecnológica. Brasil: Revista Redalyc. (Vol. 4, págs. 85-97).			

Subcategoría 1: Políticas de Accesos				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
IBM	**2012**	Las políticas de seguridad son dinámicas también, así que las soluciones de administración de identidad deben incluir herramientas que simplifican la creación de políticas y permiten a los administradores evaluar el impacto potencial de los cambios de política sin introducirlas a un entorno de producción. La conformidad y la supervisión requieren la capacidad de administrar datos de identidad y acceso. Los informes predefinidos y eventos de auditoría deben ayudar a los auditores a obtener rápidamente una visión exacta de la postura de seguridad y el estado de conformidad de una organización (p.4).	Las políticas de accesos son flexibles a la corporación, de manera que los resultados que tienen los responsables de otorgar accesos, se tienen incorporado las políticas de instrumentos para poder brindar accesos a los nuevos usuarios que tengan contacto con documentos virtuales, necesitando conformidad de los requerimientos atendidos (IBM, 2012).	En la investigación las políticas es un control que tienen que cumplir lo colaboradores en el momento de encontrarse en eventos que arriesguen la perdida de información o vulneración de datos,
Referencia:	IBM. (2012). Gestione identidades y el acceso para una continua conformidad y una reducción de riesgos. EE.UU: IBM Corporation.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Inmaculada Carrión Señor, José Luis Fernández Alemán y Ambrosio Toval	2011	Según Carrión, Fernández y Toval (2011) la políticas de accesos se: Autoriza a determinados usuarios a realizar un conjunto de acciones en un conjunto de recursos, si se cumplen unas determinadas condiciones (p.6).	La políticas de acceso consiente a definir internautas a ejercer conglomerados de encuentros unidos a ingenios, formalizando valerosos requisitos (Carrión, Fernández y Toval, 2011).	En el despliegue de la exploración las reglas o normas que se emprenden en sistemas o entidades son importantes puntos que visualizan los dictámenes del colaborador.
Referencia:	Carrión, I., Fernández, J., & Toval, A. (2011). Gestión del control de acceso en historiales clínicos electrónicos: revisión sistemática de la literatura. Barcelona: Gac Sanit. (Vol. 26, págs. 463-468).			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Myriam Cardozo Brum	2013	Según Cardozo (2013), indica que las políticas: **L**as políticas públicas constituyen respuestas diseñadas y aplicadas, a través de procesos políticos y técnicos, para resolver problemas que, por su relevancia para importantes sectores de la sociedad, no son factibles de enfrentarse eficazmente desde el ámbito privado. Ellas surgen como resultado de "...un proceso de sucesivas tomas de posición, que se	La política promulga acciones ejecutadas, a través de actividades políticas, para absolver hechos que solo son importantes en dichos sectores y no son ejecutadas en el ámbito privado. Surge como evento de un proceso, siendo compuesto por decisiones, de una entidad pública,	Acerca de la promulgación de una política, que es definida por el comité del área o el departamento, es importante activar dicha política para absolver riesgos que se está observando en una entidad bancaria o financiera, orientando

		concretan en un conjunto de decisiones, acciones u omisiones, asumidas fundamentalmente por los gobiernos, que traducen, en un lugar y período determinado, la respuesta preponderante del mismo frente a los problemas públicos vividos por la sociedad.(p.4),.	por periodo y en un lugar, frente a las situaciones que vive la población (Cardozo, 2013).	a los colaboradores de que al activar es ejecutar en el ambiente laboral.
Referencia:	Cardozo, M. (2013). Políticas públicas: los debates de su análisis y evaluación. Mexico: Andamios. (Vol. 10, págs. 39-59).			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Ciro Antonio Dussan Clavijo	2006	Según Dussan(2006)indica que las políticas: Definen la forma de hacer las cosas, el mejoramiento de los procesos. Reconocer las limitaciones y restricciones de la tecnología es un buen paso para entender la importancia de las políticas. En este sentido podemos definir la política como un instrumento gerencial que traza una dirección predeterminada describiendo la manera de manejar un problema o situación. Las políticas son planteamientos de alto nivel que transmiten a los colaboradores de la empresa la orientación que necesitan para tomar decisiones presentes y futuras. Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro y en algunos casos fuera de la organización.(p.88)	Las políticas definen el modelo para organizar las cosas y arregla los procesos. Recordar de las prohibiciones y del obstáculo de la tecnología es comprender lo primordial de las políticas. La política traza un camino para operar un evento problemático. Teniendo las políticas damos a los colaboradores medios para que tomen las decisiones que surgen en las actividades del día y mañana (Dussan, 2006).	Por lo que se refiere a las políticas que se crean en la empresa son procedimiento que tiene que seguir el colaborador ante una situación problemática, siendo estas políticas, una información importante que se tomara en una situación cotidiana y futura que tiene el empleado con la empresa.
Referencia:	Dussan, C. (2006). Políticas de seguridad informática. Lima: Revista Redalyc.			

Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Ing. Raydel Montesino Perurena, Dr. Walter Baluja García y Ing. Joelsy Porvén Rubier	2013	Según Montesino, Baluja y Porven (2013) la políticas de accesos se: se logra mediante la implantación de un grupo de controles que incluyen políticas, procedimientos, estructuras organizativas y sistemas de hardware y software (p.3)	Las políticas de acceso se alcanza interviniendo instauraciones de un conjunto de inspecciones que engloba tácticas, métodos, configuraciones administrativas y cumulo de componentes físico e ordenes que guie al procesador (Baluja y Porven, 2013).	Para la aplicación de un modelo, se requiere que intervengan auditores que reconozcan que régimen o regla exige el bosquejo, para conducir a los vínculos que poseerían los funcionarios.
Referencia:	Montesino, R., Baluja, W., & Porven, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. Cuba: Scielo.			

Subcategoría 2: Control de Accesos				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Revista Gerencia	2010	Según Revista Gerencia (2010) el control de Accesos se expresa a que: Las distintas áreas del mercado han encontrado en los sistemas de control de acceso y seguridad, aplicaciones muy útiles para monitorear la gestión y la producción (p.3).	El control de acceso manifiesta que la región del comercio ha hallado un cumulo de estatus que normaliza la marcha de la actividad con la firmeza, para vigilar la dirección (Revista Gerencia, 2010).	En el estudio propuesto el control de acceso se explaya al delegar estatus a los modelos, actividades a desarrollar.
Referencia:	Gerencia, R. (2010). Control de acceso. Chile: Revista Gerencia-Noticias, analisis e informacion. (Vol. 1, págs. 1).			

Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Arantxa Mora Perez	2016	Según Mora (2016) el control de acceso se: Requiere flexibilidad para que no haya limitaciones en la movilidad por cambios que se producen en los permisos. Necesita precisión para que se le asigne el permiso correcto a cada persona (p.10).	Notificar tolerantemente restricciones en la variación que reportar autorización, exige minuciosamente fijar anuencia apropiada de cada individuo (Mora, 2016).	Para requerir una variación de un perfil en los modelos o diseños se exige una consenso de los departamentos, para efectuar la eventualidad.
Referencia:	Mora Perez, A. (2016). Gestión de Prevención. Control de acceso. España: Repositorio Universidad Policitenica de Cartagena.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Carlos Henríquez	2010	Según Henríquez(2010) el control de accesos son: sistemas que permiten manejar una autoridad para controlar el acceso a recursos o áreas en una instalación física dada o en un sistema de información basado en computadoras (p.64).	Un cumulo de estatus que normaliza la marcha de la actividad admite a maniobrar un privilegio para comprobar la entrada de requerimientos o sectores en ubicaciones tangible o en ordenadores (Henríquez, 2010).	Para obtener un estatus que normalice con prioridad los objetivos de las tareas se requiere que tome con superioridad los controles de las conexiones que les asignan a los usuarios.
Referencia:	Henriquez, C. (2010). Sistema de control de acceso basado en Java Cards y Hardware libre. Mexico: Revista Redalyc. (Vol. 8, págs. 63-68).			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Diana Shirley Morales Tejada	2012	Según Morales (2012) el control de acceso es: la habilidad de permitir o denegar el uso de un recurso físico (áreas restringidas según rango del visitante) o virtual (acceso a información) a personas o entidades en particular. Para dar claridad al proyecto, se quiere implementar un control de acceso físico que está basado en el control de ingreso y salida en edificios, inmuebles, cuartos o áreas específicas únicamente a personas autorizadas (p.18).	Admitir o impugnar la utilización de un bien tangible o eventual a usuarias u organismos, para otorgar luminosidad al propósito, se avisa para poner en funcionamiento la intervención de ingreso tangible, que está centrado en la admisión y partida a usuarias consentidas (Morales, 2012).	Para otorgar privilegios a departamentos autorizados por comités de la entidad se admite por el logro que ha llegado ser la necesidad de la misión del plan que se va implantar en la entidad.

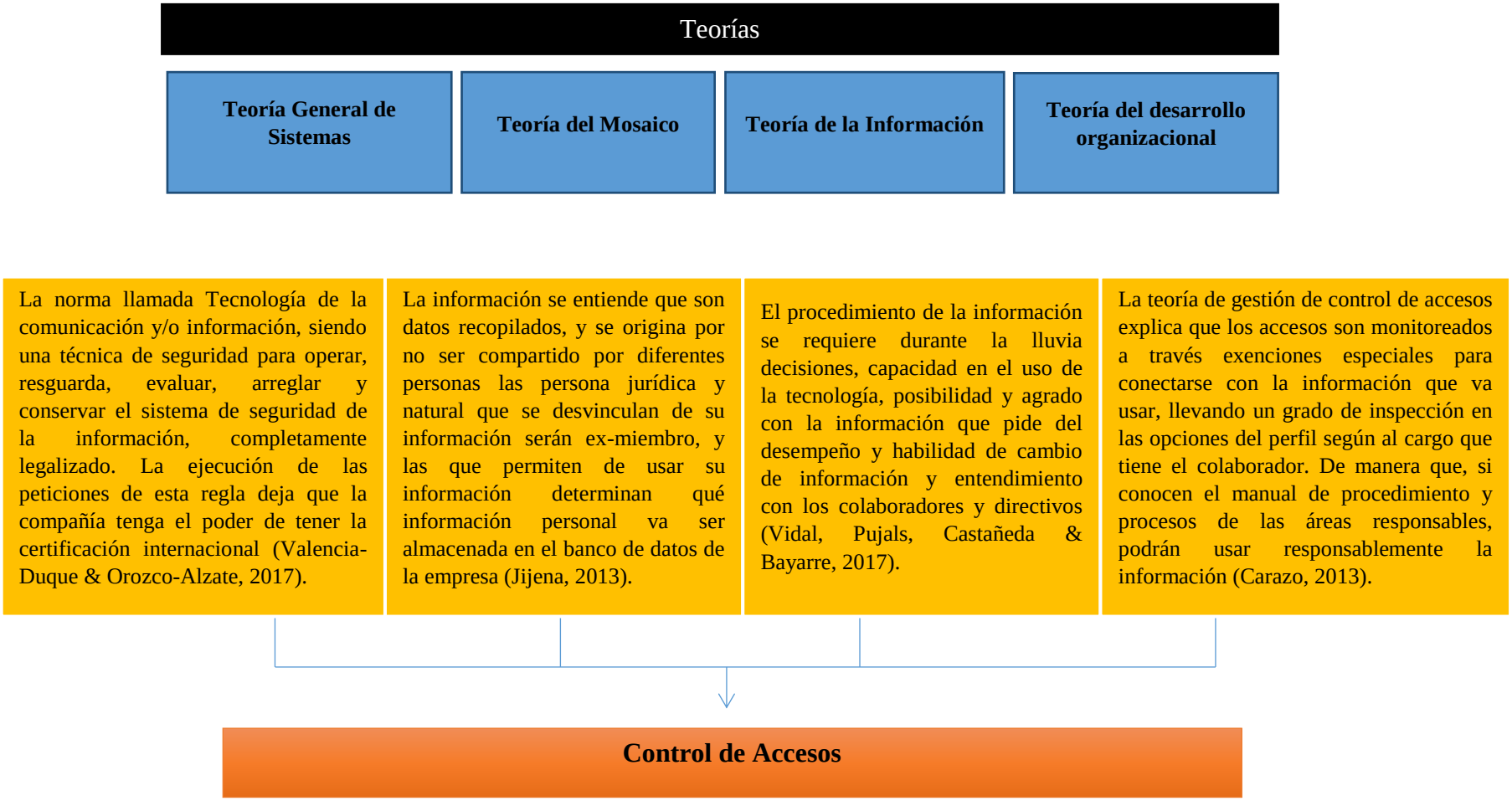
Referencia:	Morales tejada, S. (2019). Prototipo de Control de Acceso Peatonal al Campus de la Corporación Universitaria. Colombia: Corporación Universitaria Lasallista.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Dirección Nacional Seguridad y protección	2019	Según Dirección Nacional Seguridad y protección (2019) el control de acceso: Los bienes informáticos estará basado en una política de "minimo privilegio", en el sentido de otorgar a cada usuario solo los derechos y provilegios que requiere para el cumplimiento de las funciones que tenga asignadas (p.60).	Una posesión es fundamental en la erudición de la instrucción relacionado al tacto de facultar honor en los cibernautas para que efectué el desempeño que goza a cumplir (Dirección Nacional Seguridad y protección, 2019).	Basado al estudio enunciado es fundamental que el usuario tenga instrucción de los roles que debe cumplir cuando desempeñe sus funciones.
Referencia:	Dirección Nacional Seguridad, p. (2019). Metodología para la gestión de la seguridad informática. Cuba: Oficina de Seguridad para las redes informáticas.			

Subcategoría 3: Sistemas y Aplicaciones				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Giraldo Betancur Paulo Cesar	2009	Según Betancur (2009) los sistemas y aplicaciones se: Constituye una forma de entender las diferentes maneras de cómo la familia desarrolla la producción, pues éste permite visualizar los diferentes elementos que entran al predio, cómo son transformados, a través de qué procesos y, finalmente, qué resultados se obtienen o cuáles son los productos de estos procesos (p.69).	Los sistemas y aplicaciones conforma los procedimientos de comprender los diversos progresos, ya que consiente a imaginar los distintos componentes, siendo convertidos, en las sucesiones que se obtiene en los efectos de la sucesión (Betancur, 2009).	En el estudio los sistemas y las aplicaciones es fundamental ya que es para acceder e modelar nuestra propuestas necesitamos de los accesos al sistemas y aplicaciones que tiene la financiera.
Referencia:	Betancur, P. (2009). Aplicación del modelo de sistemas de producción y medios de vida a un caso rural del Departamento de Risaralda. Manizales, Caldas, Colombia: Revista Luna Azul. (Vol. 28, págs. 68-85).			

Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Luis Antonio Domínguez Coutiño	2012	Según Domínguez (2012) los sistemas y aplicaciones es: Un proceso que requiere conocer quién lo realiza, el objetivo que se pretende alcanzar y las condiciones particulares en las que se desarrolla. Sin embargo, antes de emprender el análisis de un sistema, conviene estar al tanto de la clasificación general de los sistemas (p.10).	El curso que notifica lo puede dominar, siendo neutral en lo que solicita para adquirir posición en la que se extiende, entablando una partición en la indagación del cumulo de estatus que normaliza la marcha de la actividad (Dominguez, 2012).	En el estudio notificar los incidentes que observamos en el sistemas y aplicaciones es poder conocer los vulnerabilidades que podría estar en peligro los documentos e información de la financiera.
Referencia:	Domínguez, L. (2012). Analisis de Sistema de Información. Mexico: Red Tercer Milenio.			

Autor/es	Año	Cita	Parafraseo	Aplicación en su tesis
Silvia Carrasco Usano	2015	Según Carrasco (2015) los sistemas y aplicaciones mediante: Sistemas que recogen procesos internos, pedidos, seguimientos, etc., lo cual puede llevar a aumentar la fidelización de los agentes externos con los que trata la empresa al otorgarles un fácil acceso a la información que necesiten (p.16).	Los cumulo de estatus que normaliza la marcha de la actividad recolectan fases del interior, búsqueda, entre otros, ampliando la lealtad de los representantes con los que pacta la entidad al conceder una sencilla entrada al testimonio que requiere (Carrasco, 2015).	Para el estudio el sistema tiene que poner en marcha las fases, rangos, que requiere para que tengan reglas de seguridad y poder resguardar la información de la entidad.
Referencia:	Carrasco, S. (Julio de 2015). Análisis de la aplicación de la tecnología móvil en las empresas. Obtenido de Universidad Politecnica de Valencia, España.			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Camila Santana Domingos, Gabriela Tavares Boscarol, Lídia Miranda Brinati, Alessandro Custódio Dias, Cristiane Chaves de Souza y Patrícia de Oliveira Salgado	2017	Según Santana, Tavares, Miranda, Custodio, Chaves y Oliveira (2017) los sistemas y aplicaciones se: en este escenario como mecanismos de colecta, procesamiento, análisis y transmisión de las informaciones necesarias, permitiendo la planificación, organización, operacionalización y evaluación de los servicios de salud (p.605).	Los sistemas y aplicaciones entabla con dispositivos que recauda, métodos, transferencias de los testimonios que requiere facultando el programa, estructura, manipulación y valoración de las asistencias (Santana, Tavares, Miranda, Custodio, Chaves y Oliveira, 2017).	Para elaborar un modelo en un sistema y aplicación se requiere ver que opciones va tener para ordenar sus funciones que obtendrá los colaboradores, siendo este primordial cuando acceda al sistema.
Referencia:	Santana, C., Tavares, G., Miranda, L., Custodio, A., Chaves, C., & Oliveira, P. (2017). La aplicación del proceso informático de enfermería: revisión integradora. España: Revista Electronica de Enfermeria. (Vol. 48, págs. 603-619).			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Jose Manuel Rodriguez Rodriguez y Maria Jose Daureo Campillo	2003	Según Rodríguez y Daureo (2003) los sistemas y aplicaciones son: Nuevos sistemas y plataformas más potentes a la vez que más económicas hace que muchas organizaciones se planteen el traslado de sus aplicaciones corporativas que residen en servidores centrales o mainframes hacia nuevas plataformas (p.20).	El reciente soporte más intenso y más ahorrador hace a las entidades a sugerir la extracción de sus datos o servicio que se establece en una reserva céntrico o un componente céntrico hacia novedosos propuestas (Rodríguez y Daureo, 2003).	Cuando se extrae información o data de sistemas y aplicaciones se requiere de mantener servidores de mantenimiento para restablecer los datos si no tienen los sistemas copia de seguridad.
Referencia:	Rodríguez Rodríguez, J., & Daureo Campillo, M. (2003). Sistemas de información: Aspectos tecnicos y legales. Mexico: Universidad de Guadalajara.			

7. Construcción de la categoría problema



8. Matriz del método

Sintagma				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Hurtado de Barrera, J.	2010	Según Hurtado (2010) el sintagma son : los diferentes métodos de los paradigmas en investigación, ilustrado metafóricamente por un modelo en espiral del proceso investigativo denominado espiral holística (p.118).	En la investigación el sintagma son distintos maneras de formular las estructuras de exploración, instruido por figurativos que detalla prototipo o pautas que escalonan gradualmente sucesiones que busca designar progresivamente un elemento a un modo total (Hurtado, 2010).	Nuestro estudio es sintagma holística a manera que nos proporciona la exploración de tipos, bosquejos o prototipos que permita mejorar y enriquecer de manera gradual con la investigación.
Referencia:	Hurtado de Barrea, J. (2010). Guia para la comprension holisitica de la ciencia. Venezuela: Universidad Nacional Abierta Direccion de Investigacion y Postgrado.			

Enfoque				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Roberto Hernandez	2014	Según Hernández (2014) indica que el enfoque : Se basa en métodos de recolección de datos no estandarizados ni predeterminados completamente. Tal recolección consiste en obtener las perspectivas y puntos de vista de los participantes (sus emociones, prioridades, experiencias, significados y otros aspectos más bien subjetivos).(p.8)	Se define que el enfoque son herramientas que recaudan datos no normalizados. La recaudación de datos consiste en lograr los objetivos y las ideas que fueron reevaluados por los usuarios (Hernández, 2014).	Las herramientas que nos va otorgar el apoyo de recolectar la información de los clientes, siendo una gran ayuda para cumplir los objetivos de nuestra división.
Referencia:	Hernández Sampieri, R. (2014). Metodología de la Investigación. Mexico: Mc Graw Hill Education / Interamericana Editores S.A.			

Tipo				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Daniel Cauas	2015	Cauas (2015) indica que tipo: Este tipo de estudios buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que se sometido a análisis. En un estudio descriptivo se selecciona una serie de cuestiones y se mide cada una de ellas	El tipo de modelo investiga específica los dominios principales de las personas, equipos, corporación u otra rareza que es sometido al análisis. En una instrucción descriptiva se escoge una colección de cuestiones y evalúa cada una de ellas deliberadamente, para explicar lo que investiga. El modelo de preparación nos puede otorgar un nivel de pronóstico (Cauas, 2015).	En la investigación el tipo de estudio nos va a otorgar el medio para medir el modelo o boceto que vamos a seguir para determinar una buena herramienta de solución.

		independientemente, de forma tal de describir los que se investiga. Este tipo de estudio puede ofrecer la posibilidad de llevar a cabo algún nivel de predicción (aunque sea elemental).(p.6)		
Referencia:	Cauas, D. (2015). Definición de las variables, enfoque y tipo. Francia: Calameo. (Vol. 1, págs. 1-11).			

Nivel				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Gallardo Echenique, Eliana Esther	2017	Según Gallardo (citado por Arias, 2017) indica que el nivel: El nivel de investigación se refiere al grado de profundidad con que se aborda un fenómeno u objeto de estudio".(p.53)	Se define nivel como una cota de búsqueda que refiere una categoría de profundidad que lleva a aproximarse a una rareza o elemento de enseñanza (Gallardo 2017).	En definitiva en nuestra investigación los niveles nos van a otorgar datos que podemos calificar a nivel de rangos, fases, para poder determinar un mejor objetivo en nuestra investigación.
Referencia:	Gallardo Echenique, E. (2017). Metodología de la Investigación: manual autoformativo interactivo. Huancayo, Peru: Repositorio Continental.			

Diseño				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
José Alberto Yuni Claudio Ariel Urbano	2014	Según Yuni y Urbano (2014) indica que Diseño : La elaboración del diseño de investigación consiste en ordenar una serie de componentes metodológicos con el fin de elaborar un plan lógico que organice el trabajo de campo y ayuda a evitar los sesgos.(p.10)	Se determina diseño como realización del boceto de búsqueda se basa en jerarquizar una lista de elementos metodológicos con el objetivo de realizar un plan lógico que ordene la función de actividades y es el apoyo a esquivar las inclinaciones que podemos encontrar a través del diseño (Yuni y Urbano, 2014).	En nuestra investigación el diseño es un medio de determina qué modelo podemos seguir para seguir con una jerarquización en nuestro plan de estudio que vamos ejecutar en la investigación.
Referencia:	Yumi, J., & Urbano, C. (2014). Tecnicas para investigar - Recusos Metodologicos para la prepacion de proyectos de investigación. Argentina: Editorial Brujas.			

Método				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Maya	2014	Según Maya (2014) indica que el método: El método es común a todas las ciencias, ya que se trata de un procedimiento riguroso formulado lógicamente, que permite adquirir un conjunto de	Se define método como una actividad usual a todas las ciencias, de manera que se trata de métodos inflexible formulado lógicamente, que deja conseguir un grupo	En la investigación los métodos son procedimientos lógicos que vamos a seguir, para llevar a cabo las herramientas que se va utilizar

		conocimientos en forma sistemática y organizada (p.11).	de instrucciones en un modo sistemático y organizado (Maya, 2014)	en nuestra investigación.
Referencia:	Maya, E. (2014). Metodos y tecnicas de investigación. Mexico: Universidad Nacional Autonoma de Mexico. (Vol. 1, págs. 69-74).			

9. Población, muestra y unidades informantes

Población				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Pedro Luis López	2004	Según López (2004)indica que la población es: La población es un conjunto de elementos que contienen ciertas características que se pretenden estudiar. Por esa razón, entre la población y la muestra existe un carácter inductivo (de lo particular a lo general), esperando que la parte observada (en este caso la muestra) sea representativa de la realidad (entiéndase aquí a la población); para de esa forma garantizar las conclusiones extraídas en el estudio.(p.3)	Se define población como un grupo de herramientas que tienes ciertas peculiaridades que se puede evaluar. Por ese motivo la población y muestra se califica como inductivo, siendo que la parte examinada sea objetiva de la realidad, para que se asegure formas en el resultado que se recogió en la investigación (Lopez, 2004).	La población es una herramienta fundamental para analizar el estudio que nos va determinar a una gran proporción de personas que vamos a evaluar durante el proceso de nuestra investigación.
Número de población:		**60**		
Referencia:		Lopez, P. (2004). Población, Muestra y Muestreo. Bolivia: Punto Cero. (Vol. 1, págs. 69-74).		

Muestra				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Tamara Otzen & Carlos Manterola	2017	Según Otzen & Manterola (2017) indica que la muestra en el: Una muestra puede ser obtenida de dos tipos: probabilística y no probabilística. Las técnicas de muestreo probabilísticas, permiten conocer la probabilidad que cada individuo a estudio tiene de ser incluido en la muestra a través de una selección al azar. En cambio, en las técnicas de muestreo de tipo no probabilísticas, la selección de los sujetos a estudio dependerá de ciertas características, criterios, etc.(p.5)	La muestra se define en dos modelos: probabilística y no probabilística, son métodos de muestreo probabilísticos, que nos servirán como modelo de la probabilidad que tiene cada usuario en la evaluación para ser incorporado a través de una elección aleatoria. Con las técnicas de muestreo de carácter no probabilístico, la elección del estudio es examinada por ciertas definiciones, pautas, entre otros (Otzen & Manterola, 2017).	En definitiva, la investigación es la muestra que gran parte representa la población, donde vamos a evaluar y analizar el proceso de verificación para llevar a cabo una solución a los problemas.

Técnica de muestreo:	Aleatorio
Número de muestra:	30
Referencia:	Otzen, T., & Manterola, C. (2017). Tecnicas de muestreo sobre una población a estudio.Chile: Scielo. (Vol. 35, págs. 227-232).

Unidades informantes				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Jorge Bustamante R.	2017	Según Bustamante (2017) indica que las unidades informantes: Consiste en el conjunto de actividades que, partiendo de una recogida de datos individuales, conduce a la presentación de resultados agregados en forma de tablas o de índices. Los datos individuales pueden recogerse, directamente de las unidades informantes mediante un cuestionario o juego de cuestionarios que se procesan conjuntamente.(p.82)	Es un grupo de tareas que a partir de la recolección de datos, promueve a la presentación de los resultados que están en los gráficos y tablas. La información se recoge a través de encuestas o evaluaciones que nos puede otorgar un resultado eficaz (Bustamante, 2017).	En la investigación la medida de recolectar datos a través de cuestionario o evaluación, puede otorgarnos rápidos resultados que nos podrá ayudar a un determinado grupo de colaboradores.
Número de entrevistas:		**60**		
Referencia:		Bustamante, J. (2017). Lineamientos básicos de una investigación estadística. Dirección de Regulación, Planeación,Estandarización y Normalización (DIRPEN) .		

10. Técnicas e instrumentos

Técnica/s				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Arias-Robles, F. y García-Avilés	2016	Según Roble & Aviles (2016) indica que las técnicas: Son mediante técnicas como la recopilación, la sistematización y el análisis cuantitativo y cualitativo. De este modo, a partir del estudio de la evolución de sus tendencias, elementos comunes y matices, se espera haber clarificado el significado y el alcance de un término con tanto recorrido como horizonte por delante.(p.65)	Las técnicas se caracterizan por estar como herramientas sistemáticas, en un análisis cuantitativo y cualitativo. De esta manera la evaluación va tener medidas de evaluación, para tener un buen significado a través de sus objetivos y de su alcance de término horizontal (Roble & Aviles, 2016).	En nuestra investigación las técnicas nos van apoyar como medio de herramientas que van hacer un buen uso de seleccionar mejor nuestros objetivos, propósito que debemos implementar en nuestro plan de investigación.

Referencia:	Roble, F., & Jose, A. (2016). Definiendo la hipertextualidad. Análisis cuantitativo y cualitativo de la evolución del concepto.España: Revista Dialnet. (Vol. 14, págs. 1-68).

Instrumento/s				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Simón Pedro Izcara Palacios	2014	Según Izcara (2014) define que los instrumentos son: instrumentos de acopio de datos cualitativos, establece las diferencias entre diversas técnicas y procedimientos de recogida de información, y explica los aspectos teóricos y técnicos básicos para aplicar las dos técnicas más importantes de recogida de datos cualitativos: la entrevista en profundidad y el grupo de discusión.(p.15)	Los instrumentos son recolección de datos cualitativos, que nos permite diferenciar diversas métodos y capacidades para la recogida de nuestra información, definiendo muestra teóricas y herramientas comunes que nos puede ayudar para aplicar las técnicas más importantes para la recogida de los datos, que han sido halladas a través de entrevistas y nube de ideas (Izcara, 2014).	En definitiva, los instrumentos es una parte fundamental para evaluar las técnicas de evaluación para llevar a un determinado método, que vamos a ejecutar durante la implementación de la solución.
Referencia:	Iscara, S. (2014). Manual de investigacion cualitativa. Lima, Peru: Ministerio de Educación.			

Validez				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Gustavo A. Cabrera-Arana, Jaime L. Londoño-Pimienta y León D. Bello-Parías	2008	Según Cabrera, Londoño & Bello (2008) indica que la validez es: el instrumento se revisó al interior del equipo consultor para "certificar" o " validar" si las preguntas: median lo que se quería, parecía y debían medir (apariencia); incluían los dominios y subdominios de la calidad percibida, sin los de calidad técnica o satisfacción (validez de constructo); funcionaban como otros instrumentos de percepción de calidad (validez de criterio); medían cambios en la realidad (sensibilidad al cambio) y, finalmente, si era en su conjunto un instrumento práctico, amigable, de extensión adecuada, rápido de aplicar, procesar y conservar en un archivo, para conocer la validez de su utilidad y practicidad (p.7).	La herramienta es evaluado a través del personal de la investigación, para evaluar y dar la conformidad, que los datos que van a medir y validar nuestros indicadores y objetivos de nuestra investigación. (Cabrera, Londoño & Bello, 2008)	En nuestra investigación la palabra validez es un significado que confirma que la información y datos que utilizamos son altamente confiables y claros durante los procesos de la investigación.

	Apellidos y nombres	Especialidad	Criterio de evaluación
Validador 1	Chavez Alvarado, Walter Amador	Educación	4
Validador 2	Fox Cortez, Julio Alonso	Educación	4
Validador 3	Ramos Muñoz, Alfredo Marino	Tecnología de Información	4
Referencia:	Cabrera, G., Londoño, J. & Bello, L. (2008). Validación de un instrumento para medir calidad percibida por usuarios de hospitales de colombia. Colombia: Universidad de Antioquia. Medellín.		

Confiabilidad				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Mendoza, J. & J. B. Garza	2009	Según Mendoza & Garza (citado por Cresswell, 2009) indica que la confiabilidad : Cuando se utiliza un instrumento modificado o se combinan instrumentos en un estudio, el nuevo instrumento no necesariamente refleja la validez y consistencia de los instrumentos originales, de esta manera, es muy importante volver a establecer la confiabilidad y la validez, al analizar los datos en este nuevo estudio .(p.24)	Cuando se usa una herramienta que ha cambiado los instrumentos, no nos confía la seguridad y confianza de las herramientas originales, siendo este medio para establecer una confianza en el momento de aprobar, evaluar los datos de la investigación (Mendoza & Garza, 2009)	En la investigación la confiabilidad se verifica a través de la evaluación de los datos que vamos a presentar en la investigación, reflejando que los datos que esta nuestro trabajo en son primordialmente validadas a través de herramientas estadísticos.

Prueba de confiabilidad	Alfa de Cronbach	Criterio de evaluación:	x Aplicable No aplicable
Valor calculado	0,725		
Referencia:	Mendoza, J., & Garza, J. (2009). La medición en el proceso de investigación cientifica. Mexico: Revista Universidad Autónoma de Nuevo León, Innovaciones de Negocios. (Vol. 6, págs. 17-32).		

Nro.	**Sub categoría**	**Indicador**	**Ítem**	**Cuestionario**					**Nro.**	**Guía de entrevista**		
				N	**A**	**Nt**	**CS**	**S**		**E1**	**E2**	**E3**
1	Políticas de Accesos	Disponibilidad	¿Cuándo un trabajador comienza a elaborar y asumir sus funciones se le otorgan sus respectivos usuarios al sistema de la financiera?	**1**	**2**	**3**	**4**	**5**	**1**	¿Cómo es el proceso para que los colaboradores tengan sus accesos en el sistema, y que se requiere para obtener la disponibilidad de información que no tiene a su cargo?	¿Cómo es el proceso para que los colaboradores tengan sus accesos en el sistema, y que se requiere para obtener la disponibilidad de información que no tiene a su cargo?	¿Cómo es el proceso para que los colaboradores tengan sus accesos en el sistema, y que se requiere para obtener la disponibilidad de información que no tiene a su cargo?
			¿Solicita permisos para ingresar a información secreta, confidencial y interna que no tiene que ver con su cargo?	**1**	**2**	**3**	**4**	**5**				

		Seguridad	¿Los colaboradores cumplen con los controles de acceso de seguridad cuando manejan la información de los clientes?	**1**	**2**	**3**	**4**	**5**	**2**	¿Qué realiza el área de seguridad de información para que la financiera y los colaboradores cumplan con las políticas de seguridad?	¿Qué realiza el área de seguridad de información para que la financiera y los colaboradores cumplan con las políticas de seguridad?	¿Qué realiza el área de seguridad de información para que la financiera y los colaboradores cumplan con las politicas de seguridad?
			¿Considera Ud. Que la financiera cumple con las políticas de seguridad de información para salvaguardar la información?	**1**	**2**	**3**	**4**	**5**				
		Accesos de Seguridad	¿Considera Ud. que los accesos que se le otorgan a los colaboradores tengan restricciones de seguridad?	**1**	**2**	**3**	**4**	**5**	**3**	¿La empresa como controla los accesos del colaborador y de los proveedores cuando usa la información y como definen uds. La restricciones que debe tener cada cargo?	¿La empresa como controla los accesos del colaborador y de los proveedores cuando usa la información y como definen uds. La restricciones que debe tener cada cargo?	¿La empresa como controla los accesos del colaborador y de los proveedores cuando usa la información y como definen uds. La restricciones que debe tener cada cargo?
			¿Que la información que usas tienen controles de seguridad en los sistemas y aplicaciones de la empresa?	**1**	**2**	**3**	**4**	**5**				
			¿Cuándo se le otorga acceso a los jefes y los proveedores crees que se le debe restringir los accesos que no están a su cargo?	**1**	**2**	**3**	**4**	**5**				
2	Control de Accesos	Compromiso con los colaboradores	¿Ha recibido alguna documentación donde se comprometa a usar con responsabilidad la información que maneja y usa en el sistema de la empresa?	**1**	**2**	**3**	**4**	**5**	**4**	¿Por qué se considera necesario que los colaboradores y proveedores firmen el compromiso de confiabilidad de información?	¿Por qué se considera necesario que los colaboradores y proveedores firmen el compromiso de confiabilidad de información?	¿Por qué se considera necesario que los colaboradores y proveedores firmen el compromiso de confiabilidad de información?
			¿Los proveedores cuando inician un contrato con la financiera firman un contrato de confiabilidad?	**1**	**2**	**3**	**4**	**5**				

		Medidas de accesos	¿Cuándo se le otorga acceso a los colaboradores se requiere de alguna conformidad del jefe o gerente encargado?	**1**	**2**	**3**	**4**	**5**	**5**	¿En qué momento se solicitad conformidad para tener accesos a los sistemas?	¿En qué momento se solicitad conformidad para tener accesos a los sistemas?	¿En qué momento se solicitad conformidad para tener accesos a los sistemas?
			¿Cuándo comparten documentos confidenciales a proveedores o a la SBS, se requiere de conformidad del jefe o gerente?	**1**	**2**	**3**	**4**	**5**				
		Inducción	¿Ha recibido inducción sobre el manejo de la información cuando accede al sistema de la empresa?	**1**	**2**	**3**	**4**	**5**	**6**	¿Cuáles son los temas que exponen en la inducción a los colaboradores y a que personal de la financiera orienta sobre seguridad de información?	¿Cuáles son los temas que exponen en la inducción a los colaboradores y a que personal de la financiera orienta sobre seguridad de información?	¿Cuáles son los temas que exponen en la inducción a los colaboradores y a que personal de la financiera orienta sobre seguridad de información?
			¿Considera ud. Que se debería orientar a los colaboradores acerca de las responsabilidades que tiene el usuario cuando usa información de la empresa?	**1**	**2**	**3**	**4**	**5**				
3	Sistemas y Aplicaciones	Uso	¿Todos los sistemas que usa el colaborador tienen definidos los roles y perfiles según los cargos que tiene?	**1**	**2**	**3**	**4**	**5**	**7**	¿Cómo definen uds. Que rol le corresponde al perfil que tiene uso el colaborador en el sistema de la empresa?	¿Cómo definen uds. Que rol le corresponde al perfil que tiene uso el colaborador en el sistema de la empresa?	¿Cómo definen uds. Que rol le corresponde al perfil que tiene uso el colaborador en el sistema de la empresa?
			¿Los sistemas que manejan los colaboradores tienen un usuario clave y contraseña?	**1**	**2**	**3**	**4**	**5**				
		Accesos	¿Considera ud. Que los controles no automatizados que tienen la empresa son de utilidad para verificar los accesos indebidos?	**1**	**2**	**3**	**4**	**5**	**8**	¿Cuáles son las controles de acceso a los sistemas y aplicaciones que maneja el área y que pasos tiene que seguir para tener accesos a otra sistema que no está a mi cargo?	¿Cuáles son las controles de acceso a los sistemas y aplicaciones que maneja el área y que pasos tiene que seguir para tener accesos a otra sistema que no está a mi cargo?	¿Cuáles son las controles de acceso a los sistemas y aplicaciones que maneja el área y que pasos tiene que seguir para tener accesos a otra sistema que no está a mi cargo?
			¿ Para obtener accesos a los sistemas y aplicaciones que no están asignados según mi cargo, se requiere de la autorización de mi jefe o gerente?	**1**	**2**	**3**	**4**	**5**				

		Monitoreo	¿Se realiza un adecuado monitoreo de los accesos que se le otorgan a los colaboradores de la empresa?	**1**	**2**	**3**	**4**	**5**	**9**	¿Qué beneficios tendría la financiera si usa herramientas para monitorear el control de accesos de la empresa?	¿Qué beneficios tendría la financiera si usa herramientas para monitorear el control de accesos de la empresa?	¿Qué beneficios tendría la financiera si usa herramientas para monitorear el control de accesos de la empresa?
			¿Ha observado ciertas irregularidades en el momento que los colaboradores usen la información de los clientes?	**1**	**2**	**3**	**4**	**5**				
			¿Recibe la empresa un informe diariamente?	**1**	**2**	**3**	**4**	**5**				

11. Procedimiento

Paso 1	Selección del tema y de la entidad que se va investigar.
Paso 2	Tener claro los objetivos que se va cumplir durante el proceso del estudio.
Paso 3	Definir las teorías que se va seguir para llevar a cabo nuestra investigación.
Paso 4	Identificar antecedentes referentes a nuestra investigación.
Paso 5	Definir si el muestreo va ser aleatorio o por conveniencia.
Paso 6	Buscar las categorías problema, las subcategorías y los indicadores
Paso 7	Formular las preguntas para el cuestionario y la entrevista
Paso 8	Realizar el vaciado de las entrevistas y el cuestionario
Paso 9	Utilizar el programa Atlas.ti para el análisis de los datos de la entrevista y el cuestionario
Paso 10	Realizar en el programa la triangulación mixta, con los análisis de la entrevista y el cuestionario

Paso 11	Realizar el Pareto, identificamos los problemas primordiales según los sustentos de los encuestados.
Paso 12	Identificar los problemas de la financiera, señalar los objetivos de la propuesta.
Paso 13	Identificar los productos para llevar a cabo la solución de los problemas.
Paso 14	Realizar los ingresos y egresos que tiene que realizar la financiera.
Paso 15	Señalar la conclusión y sugerencias.

12. Análisis de datos

Cuantitativo				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Manuel Canales Ceron	2006	Según Canales (2006)indica que cuantitativo es: Un estudio de distribución de valores de una variable en una población de individuos, trabaja con unidades simples y equivalentes. Tanto en la muestra como en el instrumento, opera con números. Individuos –abstraídos de sus relaciones sociales, y abstraídos de su complejidad subjetiva– y variables –abstraídas de las totalidades de las que forman parte– son numerables precisamente por su alto grado de abstracción (p.13).	El método cuantitativo se asigna de elementos de una variables en una población de usuarios o clientes, que estudia con unidades básicas, en la muestra y en la herramientas se trabaja con números. Los números o individuos son agarrados totalmente por una gran categoría de abstracción (Canales, 2006).	En la investigación el método nos otorgara una gran variante de beneficios para recolectar datos o información de determinados grupo de individuos.
Referencia:		Canales, M. (2006). Metodología de investigación social. Chile: LOM ediciones.		

Cualitativo				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Felipe Mora Arellano	2002	Según Mora (2002) indica que cualitativo se: Destacan las bondades y utilidad de los métodos y técnicas cualitativos, los cuales posibilitan la obtención de información difícil de obtener por otros medios, o a los cuales se recurre cuando se quiere explorar a profundidad procesos y realidades complejas, o en problemas emergentes, ámbitos novedosos o poco conocidos (p.3).	El método cualitativo destaca por elementos que se implementan en las herramientas y procedimientos cualitativos, los cuales los datos son complicados de descubrir o los hallamos por diferentes procesos y realidades difíciles de alcanzar, por ser muy poco encontrados (Mora, 2002)	En la investigación el método cualitativo es la recolección de datos que se determina a través de actividades naturales que vamos a observar durante el transcursos de agrupas las respuestas a nuestra solución.
Referencia:		Mora, F. (2002). Antología de métodos cualitativos en la investigación social. Revista Región y Sociedad. (Vol. 14, págs. 236-240).		

Mixto				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Sandra Milena Díaz López	2014	Según Díaz (citado Creswell y Plano, 2014) indica que los métodos mixtos es: Los métodos mixtos son un diseño de investigación tanto con unos presupuestos epistemológicos como con unos métodos de investigación. Como metodología supone presupuestos filosóficos que orientan la recolección y análisis de datos y la combinación de aproximaciones cualitativas y cuantitativas en muchas fases del proceso de investigación. Como método, se enfoca en la recolección, análisis y combinación de datos cualitativos y cuantitativos en un estudio o una serie de estudios (p.12).	La determinación de mixto es un modelo de estudio que se evalúa con norma de investigación. El método que orienta en la recolección, evaluación y modificación de datos, se va llevar a diferentes fases de procesos cualitativos y cuantitativos en una investigación o lista de conocimientos (Díaz, 2014).	En la investigación el modelo mixto es un método donde se combina el modelo cuantitativo y cualitativo, orientándose a varias rangos de calificación para el análisis y recolección de datos.
Referencia:	Diaz, S. (2014). Los métodos mixtos de investigación: presupuestos generales y aportes a la evaluación educativa. Portugal: Revista Portuguesa de Pedagogia. (Vol. 48, págs. 7-23).			