UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

Escuela Profesional de Ingeniería de Sistemas y Computación

TESIS

Modelo de buenas prácticas aplicando Iso 27002 para gestión de incidencias de la red Wncor.

PRESENTADO POR:

Bach. En Ing. de Sistemas y computación

Sandoval Fernández Ledy Ruth

Línea de Investigación Institucional:

Nuevas Tecnologías y procesos

Línea de Investigación por Programa de Estudios:

Ingeniería e infraestructura

PARA OPTAR TÍTULO PROFESIONAL DE:

INGENIERA DE SISTEMAS Y COMPUTACIÓN

LIMA – PERÚ

2019

UNIVERSIDAD PERUANA LOS ANDES
FACULTAD DE INGENIERÍA
Escuela Profesional de Ingeniería de Sistemas y Computación

TESIS

Modelo de buenas prácticas aplicando Iso 27002 para gestión de incidencias de la red Wncor.

PRESENTADO POR:

Bach. En Ing. de Sistemas y computación

Sandoval Fernández Ledy Ruth

PARA OPTAR TÍTULO PROFESIONAL DE:

INGENIERA DE SISTEMAS Y COMPUTACIÓN

LIMA- PERÚ

2019

ASESORES

ASESOR METODOLOGICO

MG. ANSELMO VALENZUELA ZEGARRA

ASESOR TEMÁTICO

ING. MABEL YGNACIO GARCÍA

DEDICATORIA

El presente proyecto está dedicado de todo corazón a mis padres, quienes me brindaron todo su apoyo incondicional durante estos meses otorgándome la fuerza para no rendirme y quienes son mi principal motivo para llegar a todas mis metas y a mi Valentina, mi sobrina, mi otro corazón.

AGRADECIMIENTO

A los docentes de la Universidad Peruana los Andes por brindarme sus conocimientos durante los años de estudio, agradecimiento también a compañeros y amigos que me animaron siempre a pesar de las adversidades y a las personas que de alguna manera colaboraron en esta investigación les expreso mi profundo agradecimiento.

JURADOS DE SUSTENTACIÓN

_____

PRESIDENTE

Dr. Casio Aurelio Torres López

_____

PRIMER JURADO

_____

SEGUNDO JURADO

_____

TERCER JURADO

_____

SECRETARIO DOCENTE

Mg. Miguel Ángel Carlos Canales

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE ANEXOS

RESUMEN

La presente investigación dio respuesta al problema general "¿De qué manera el modelo de buenas prácticas aplicando ISO 27002 mejorará la gestión de incidencias de la red Wncor?", el objetivo general fue "Implementar un modelo de buenas prácticas aplicando ISO 27002 para mejorar la gestión de incidencias de la red Wncor; y la hipótesis general que se contrastó fue "La Implementación un modelo de buenas prácticas aplicando ISO 27002 mejorará la gestión de incidencias de la red Wncor."

El método de investigación fue el científico, el tipo de investigación fue aplicada, el nivel de investigación fue correlacional, el diseño de la investigación fue pre experimental, se trabajó con una población que fue de 500 usuarios de los cuales se tomó un muestreo probabilístico de 40 usuarios.

Finalmente se llegó a la conclusión general: Con la implementación del modelo de buenas prácticas aplicando ISO 27002 mejoró la gestión de incidencias de la red Wncor.

Palabras claves: Modelo de buenas prácticas, Norma ISO 27002, Gestión de incidentes.

ABSTRAT

The present investigation responded to the general problem "How will the model of good practices applying ISO 27002 improve the management of incidents of the Wncor network?", The general objective was "Implement a model of good practices applying ISO 27002 to improve the Wncor network incident management, and the general hypothesis that was contrasted was "The implementation of a model of good practices applying ISO 27002 will improve the management of Wncor network incidents."

The research method was the scientist, the type of research was applied, the level of research was correlational, the design of the research was pre-experimental, we worked with a population that was 500 users of which a probabilistic sampling of 40 users

Finally, the general conclusion was reached: With the implementation of the good practice model, applying ISO 27002 improved the incident management of the Wncor network.

Keywords: Model of good practices, ISO 27002, Incident management.

INTRODUCCIÓN

En la actualidad y a nivel mundial, los temas relevantes en las empresas es establecer metodologías para restablecer la seguridad de la información, se tiene conocimiento que muchas instituciones, tanto públicas y privadas tienen más a invertir su dinero en temas de infraestructura para maquillar o cubrir las necesidades que las empresas necesitan en el momento sin buscar una estrategia para después darse cuenta que sufrieron grandes pérdidas económicas.

En muchas empresas tampoco se ha tomado importancia al método de trabajo que tienen a diario sus colaboradores, casos que a corto o largo plazo terminan afectándolos como organización, ya que estas acciones cotidianas causan retrasos a sus colaboradores sin que ni siquiera la organización pueda saberlo, haciendo que el usuario busque otro recurso que pueda ayudarlo de forma inmediata, pero muchas veces la ayuda puede no ser buena, de lo contrario, quizás cause más daños por la manipulación sin conocimiento.

Por otro lado, también se han desarrollado muchas metodologías para atender estas necesidades, entre ella la más aplicada a las empresas es la Norma ISO 27002 que hace referencia a un Sistema de Gestión de Seguridad de la Información (SGSI), cuyo objetivo es resguardar la información de la organización a través de buenas prácticas que se le debe concientizar al colaborador.

El banco Interbank conocido a nivel Internacional a pesar de su buena organización financiera y administrativa ha descuidado su enfoque directo a sus usuarios, no le toma mucha importancia porque ya cuenta con la Mesa de Ayuda que le brinda el Centro de servicios, por ello creen que todo tipo de incidencia debe ser resuelta por la Mesa. Sin embargo, hay muchos de los sucesos que pueden ser evitados por los mismos usuarios si opta por tomar la Norma ISO 27002.

Capítulo I: Se describe la problemática del proyecto, los principales motivos de las incidencias que presentan los usuarios y como les afecta en el día a día junto con los problemas que éstos causan para la empresa Interbank. También mencionamos la formulación del problema, el problema general y específicos que buscamos solucionar al finalizar el proyecto. Se describen las justificaciones del por qué estamos investigando, las delimitaciones donde se trabajará, el tiempo que nos tomó realizar todo el proyecto y qué parte especifica estamos investigando, así también describe las limitaciones que se tuvo para sacar algunas informaciones del banco sin que se piense que se está robando información y lograr sacar los resultados.

Capítulo II: Se encuentra el marco teórico, donde se encuentra toda la información que nos fue útil para la investigación, eligiendo los antecedentes que se acomodan a nuestra investigación para recopilar información importante. Así como la búsqueda de información teórica que también ayudó a seguir el procedimiento del manejo de la gestión de incidencias y aplicación de la ISO 27002. En el presente capítulo también anunciamos la hipótesis planteada según los resultados que se obtienen y que se cumplen con todo el procedimiento que se aplicó.

Capítulo III: Describimos la metodología que se utilizó para la investigación, el diseño, la muestra, las técnicas e instrumentos que se utilizaron y aplicaron para obtener los resultados. Gracias a todo lo mencionado fue posible obtener conocimientos de nuevas teorías.

Capítulo IV: Mostramos los resultados de la investigación aplicando las técnicas e instrumentos que nos ayudaron a procesar la información para saber el nivel de correlación que se tuvo entre todos los indicadores y con ello elegir las normas apropiadas según la ISO 27002 para que sean aplicadas en los usuarios de Interbank y reducir incidencias con Wncor.

Capítulo V: Encontramos la discusión de los resultados, conclusiones y recomendaciones según nos muestran los resultados, demostrando que se cumplen las hipótesis.

Finalmente se tienen las conclusiones de los resultados, recomendaciones, referencias bibliográficas y anexos.

Bach. Ledy Ruth Sandoval Fernández

CAPITULO I:
EL PROBLEMA DE INVESTIGACION

1.1. Planteamiento del problema

Una de principales molestias de los usuarios de IBK es el retrazo de sus actividades por incidentes constante que presentan dentro de la red del banco, los usuarios tienen dos principales formas de iniciar sesión al dominio que son la red físca y la red inalámbrica Wncor. Ambas redes tienen los mismos privilegios la unica diferencia es que la red Wncor es factible para que los usuarios puedan trasladarse a cualquier sede del banco utilizando una Laptop, Tablet, MAC y con ésta conexión realizar sus actividades. Pero a pesar de ser muy útil tambien muchos usuarios presentan diferentes incidentes para conectarse y una vez que ya están conectados, sin explicación presentan sus inconvenientes a pesar que un día anterior o en menos de una semana indicaban que estando conectados no presentaban esos problemas.

Los principales inconvenientes que presentan los usuarios son: Problemas para conectarse a la red Wncor y problemas para el ingreso a los File Server (Carpetas Compartidas a nivel de servidor). Estos problemas trae mucho malestar a los usuarios ya que al no lograr conectarse no es posible realizar ningun tipo de trabajo con sus equipos ya que no pueden trabajar fuera del dominio del banco, perdujicando y retrazando asi sus actividades lo que los conlleva a llamar al Centro de Servicios quienes les brindan un primer soporte por medio telefónico realizando descartes para ayudarlos con el ingreso, pero muchas veces no es posible y esto lleva al Centro de servicios a generar un ticket de atención al segundo Nivel para revisión presencial

Técnica y si a pesar de que el Segundo Nivel no logra solucionar el problema se deriva a un Tercer Nivel que es el área de Infraestructura encargado de las redes para revisar si existe un problema entre el equipo y la red.

Todo este procedimiento no es posible solucionarlo en un par de horas o un día, muchas de las incidencias demoran hasta semanas en solucionarse y estos días de esperan generan muchas perdidas miles de soles y hasta demandas al banco, ya que al no lograr conectarse los usuarios no pueden avanzar sus actividaes ni enviar sus trabajos en el tiempo esperado.

Se ha descrito los problemas mas criticos que se presentan en los usuarios del banco, pero la causa raiz de estos inconvenientes es la mala practica que tienen los usuarios para conectarse a la red Wncor, ya que los mismos usuarios por facilidades, veneficios propios o desconocimiento realizan actividades que el banco aun no ha puesto un alto o aplicado una política que conzcan los usuarios para cuidar la información, es por ello que se busca concientizar a los usuarios a no ser tran vulnerables al momento de utilizar sus equipos, ya que las principales causas es que los usuarios prestan sus equipos brindando sus contraseñas a otros usuarios, dejan sus equipos sin bloquear dejando vulnerable su información, instalan software descargados de internet sin ser licenciados por el banco o cosas muy simples como no darse cuenta de la fecha en que expiró su contraseña o haberla cambiado pero no recordar la nueva contraseña, estar conectados con cable de red y Wncor al mismo tiempo, haber reiniciado o apagado su equipo sin desconectarse de la Wncor, etc. Con estas actividades se tiene

muchos riesgos de perdida de información, vulnerabilidad de datos, clonación de contraseñas, infección del Malware, entre otros.

Todas estas malas practicas mencionadas es la causa de los problemas con la red Wncor, ya que el usuario al haber prestado su equipo esa otra persona realizó manipulaciones en su pc que no fueron infirmadas al usuario propietario, al escargar un maldware bloqueo el acceso a la Wncor, al no fijarse la fecha en que expira su contraseña o no recordarla no pueden conectarse a la Wncor por que su ingreso es con el usuario y clave de red del mismo usuario, al estar conectado por clave de red y por Wncor genera trafico de datos que hace que se bloquen algunos accesos o haber reiniciado o apagado sin desconectarse ya posiblemente el usuarios tenga otra red Wifi en su domicio y el tipo de protocolo es diferente que hace que se desconfigure de la Wncor la proxima vez de su ingreso.

1.2. Formulación y sistematización del problema

1.2.1. Problema general

- ¿De qué manera el modelo de buenas prácticas aplicando ISO 27002 mejorará la gestión de incidencias de la red Wncor?

1.2.2. Problemas específicos

a) ¿En qué medida el modelo de buenas prácticas aplicando ISO 27002 reducirá los problemas de conexión de la red wncor?

b) ¿En qué medida el modelo de buenas prácticas aplicando ISO 27002 reducirá los problemas de ingreso a los file server?

1.3. Justificación

1.3.1. Social o Práctica:

La gestión de incidencias aplicando la norma ISO 27002 para el proyecto fueron de total ayuda para los usuarios de Interbank, con la finalidad de solucionar sus incidentes y molestias diarias que causan conflictos muchas veces entre ellos y con la mesa de ayuda, mostrando sus molestias por no tener una solución inmediata que pueda salvarlos de una incidencia grave y que esta pueda causar grandes pérdidas económicas. La norma encaja positivamente en los incidentes ya que ésta se basa en las buenas prácticas para la gestión de la seguridad de la información y enseña a los usuarios la forma correcta de utilizar sus equipos para no presentar incidencias que ponen en riesgo la información de la Organización.

1.3.2. Metodológica

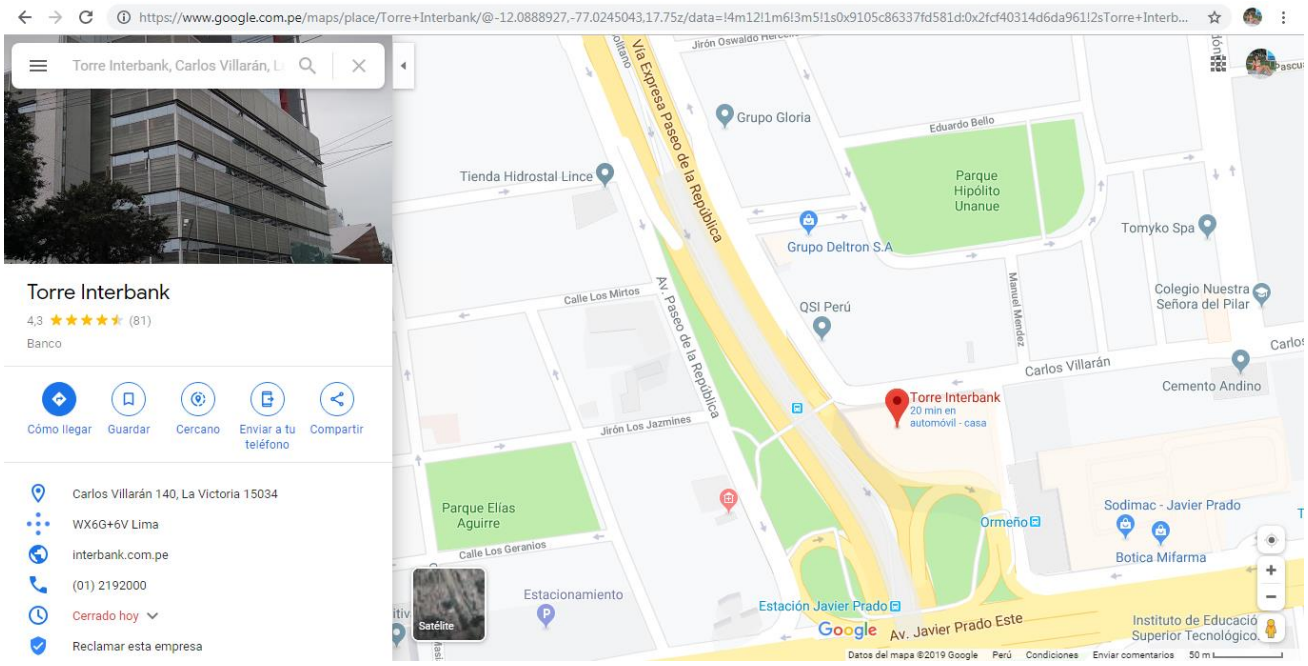
La metodología utilizada para la presente tesis se basa en el uso de un modelo de buenas prácticas que fueron aplicadas de acuerdo a las políticas establecidas en la Norma ISO 27002, quien enseña a los usuarios la manera correcta del uso cotidiano de sus herramientas laborares reduciendo las incidencias que los usuarios ocasionan y a la vez resguarda y garantiza la seguridad de información de la organización.

La aplicación de la norma ISO 27002 garantiza: seguridad, confidencialidad, disciplina, accesibilidad y disponibilidad para que cualquier organización pueda aplicarla y mantener la integridad de la misma.

1.4. Delimitaciones

1.4.1. Espacio:

El proyecto será aplicado en la sede de Interbank Torre ubicado en Carlos Villarán 140, La Victoria 15034. Se eligió ésta Sede por ser la que cuenta con mayor candidad de usuarios que tienen accesos a la Red Wncor.



1.4.2. Temporal:

El proyecto será investigado el año 2019 en un periodo de 4 meses y las muestras serán tomadas del mes de marzo filtrando tickets de las incidencias registradas por Wncor y File Server presentadas en ese tiempo, sacadas del CA Service Desk Manager que utilizaremos como uno de los instrumentos.

1.4.3. Contenido:

De todas las incidencias que se presentan con la red Wncor el proyecto será investigado sólo considerando las incidencias de ingreso a Wncor y de File server que son las mas comunes y mas reclamadas por los usuarios de interbank.

1.4.4. Económica:

La presente investigación se realizó por financimiento propio, con recursos que se pudieron obtener de Interbank de acuerdo a la necesidad que se requirió para el estudio y el logro de la finalización de la investigación.

1.5. Limitaciones

- Conseguir con total libertad una mayor cantidad de usuarios para obtener una gran muestra

- Lograr realizar el total de las encuestas dentro de la institución, por lo que algunas encuestas se tuvieron que realizar fuera de la sede, dentro de reuniones de integración, pero seleccionando sólo a usuarios con accesos.

- Ingresar a la sede para conocer las áreas más afectadas o consultar a los usuarios directamente la forma de uso de la red Wncor.

- Muchas de las consultas se realizaron por medio del Chat utilizando el Skype que se utiliza en Interbank de manera interna para realizar consultas adicionales a los usuarios.

- Realizar otras observaciones sin intención de que Interbank piense que se está robando información.

1.6. Objetivos

1.6.1. Objetivo General

- Implementar un modelo de buenas prácticas aplicando ISO 27002 para mejorar la gestión de incidencias de la red Wncor.

1.6.2. Objetivos Específicos

a) Analizar como el modelo de buenas prácticas aplicando ISO 27002 reduce los problemas de conexión de la red Wncor.

b) Indagar en qué medida el modelo de buenas prácticas aplicando ISO 27002 reduce los problemas de ingreso a los file server de la red Wncor.

CAPITULO II
MARCO TEORICO

2.1. Antecedentes

Antecedentes Internacionales

a) Daniel R. y Joffre V. (2014) "Análisis e implementación de la Norma ISO 27002 para el departamento de sistemas de la universidad Politécnica Salesiana de la Sede Guayaquil". Tesis, Guayaquil, Ecuador. Los activos de información son recursos que presentan una gran importancia y costos vitales para la universidad Politécnica Salesiana sede Guayaquil. Si estos activos llegaran a faltar o tener un daño, quedaría fuera de línea en negocio en especial en horarios con los que los sistemas de procesamiento de información intervienen y por tal razón la Universidad Politécnica Salesiana tiene el deber y obligación de preservarlos, utilizarlos y mejorarlos. Esto implica que, para tomar acciones apropiadas sobre la Seguridad de la información y los sistemas informáticos, estas decisiones deben ser basadas en la protección de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción se servicio, accidentes y desastres naturales que todos los activos expuestos.

La finalidad del Manual de Políticas de seguridad de la Información que se desea implementar en este proyecto es proporcionar instrucciones específicas sobre cómo proteger los activos de la Universidad politécnica Salesiana ya sean estos computadores de la organización (conectadas o no), como toda información guardada en ellos. La violación de dichas políticas está sujeta a medidas disciplinarias e incluso el despido.

b) Miguel L. Diseño de los procesos de gestión de incidencias y service desk, alineado a las buenas prácticas de Itil, aplicado a la empresa delltex industrial S.A. Tesis, Pontífica Universidad Católica del Ecuador, Quito; Ecuador. Delltex Industrial S.A. es una empresa textil con más de 50 años de vida y su interés en permanecer como líder en el mercado hace que la implantación de esta disertación sea una herramienta efectiva para mantener a sus clientes y para que su manejo de incidencias sea más eficiente sobre todo en el trato al cliente.

Al no tener actualmente una gestión de incidencias adecuada, Delltex Industrial S.A. no puede medir el porcentaje de satisfacción de los clientes de igual manera el tiempo de respuesta en caso de reportar un incidente repetitivo es mayor si no atiende el técnico que lo resolvió inicialmente ya que no guardan un repositorio con las incidencias y solución a las mismas.

Es necesario medir el grado de satisfacción de los usuarios o clientes internos, manejando indicadores (indicadores de los niveles de atención), para asegurar el mejoramiento continuo en Delltex Industrial S.A.

Si bien el módulo CRM de Open Orange contratado por Delltex Industrial puede parametrizarse para que funcione adecuadamente el Service desk y la Gestión de incidencias al hacer el escalamiento de forma manual deja la posibilidad de que el incidente no cierre su ciclo.

Antecedentes Nacionales

c) Samuel G y Luis T. (2018) “Implementación de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte”. Tesis, Lima; Perú. La implementación de los controles de la ISO/IEC 27002:2013 mejoró significativamente el nivel de seguridad de la información, puesto que durante la primera evaluación se obtuvo un resultado inicial de 47% y en la segunda evaluación ya con los controles implementados se obtuvo un resultado de 84%. Donde concluyó que la diferencia encontrada entre ambos resultados, mejoró en un 37% de la seguridad física y lógica de la información.

   La auditoría inicial permitió conocer cuáles son las fallas de los procesos del área de TI. Esto requiere que se implemente los controles de la ISO/IEC 27002: 2013 mejorando los procesos del negocio, haciendo que se tenga un mejor control de sus funciones.

   El desarrollo del análisis de riesgo permitió identificar que controles de la ISO/IEC 27002: 2013 se asocia al riesgo detectado, lo que implica que el riesgo cuyo valor de criticidad en nivel alto, sea tratado con mayor importancia.

   La elaboración del plan de tratamiento de riesgo permitió implementar los controles de la norma ISO/IEC 27002:2013 identificados, las cuales redujeron el impacto que ocasionan los riesgos en el área de TI, para de esta manera tener íntegra y segura a la información.

   La auditoría posterior que se realizó con los controles de la ISO/IEC 27002:2013, permitió conocer si la organización cumple con el objetivo, la cual consistió en mejorar la seguridad física y lógica de la información.

d) Roberto E. (2016) “Implementación de la norma ISO/IEC 27002:2013, sección control de acceso para las aplicaciones informáticas de la aseguradora del sur.” Tesis, Lima; Perú. El presente contiene la política de seguridad de la información que define el accionar del personal, sus responsabilidades y la revisión y/o actualización de la misma. De igual manera, contiene políticas y procedimientos que guiarán al personal de seguridad de la información para el establecimiento de accesos hacia las aplicaciones y sistemas para el establecimiento de accesos hacia las aplicaciones y sistemas en la Aseguradora del sur basado en el Estándar ISO/IEC 27002:2013; es decir, se puede encontrar los procedimientos adecuados para establecer un acceso seguro orientado a cumplir los estándares de seguridad internaciones garantizando la confidencialidad, integridad y disponibilidad de la información.

   Las disposiciones establecidas en este documento deben incorporarse como parte d las actividades normales de los colaboradores y aplicarse también en las relaciones con terceros.

e) Janet G. (2015) Implementación del marco de trabajo itil v.3.0 para el proceso de gestión de incidencias en el área del centro de sistemas de información de la gerencia regional de salud Lambayeque. Tesis, Lima; Perú. Con la implementación de las herramientas basadas en el marco de trabajo ITIL v3.0, para la gestión de incidencias de TI, se logró aumentar el número de incidencias resueltas con impacto sobre el usuario o negocio, esto gracias a que se desarrollaron procedimientos estandarizados y fáciles de entender que apoyaron la agilidad en la atención, logrando así que los encargados responsables de TI del área del Centro de Sistemas de Información (CSI) brindaran y cumplieran con todos los servicios que solicitaban los trabajadores de las diferentes áreas que conforman la Gerencia Regional de Salud (GERESA).

Gracias a la implementación del marco de trabajo ITIL v3.0, se logró reducir el tiempo destinado a la atención de las incidencias de las TI, esto se llevó a cabo gracias a la estandarización de los procesos, lo cual permitió que los encargados responsables de TI del área del CSI, agilizaran la atención de las mismas, permitiéndoles cumplir con los objetivos de TI de la Gerencia Regional de Salud (GERESA).

A través de la incorporación de ITIL v3.0, se redujo los tiempos de solución de las incidencias de las TI, esto se logró gracias a que los encargados responsables de TI del área del CSI gestionaron de la mejor manera posible las incidencias de TI que reportaban los trabajadores de la GERESA.

2.2. Marco conceptual

POLÍTICAS DE SEGURIDAD

Para López (2012). Enlace, Políticas de Seguridad "La política de seguridad es un conjunto de reglas, leyes y prácticas que regulan la forma de proteger, dirigir y distribuir recursos en una organización con la finalidad de llevar a cabo todos los objetivos de seguridad de información de seguridad dentro de la misma".

Las políticas de seguridad indican lo que no está prohibido y lo que está permitido, define las herramientas y procedimientos que son necesarias, permiten acostumbrar una buena disposición dentro de la organización y expresan el consenso de los "dueños".

De acuerdo a (Daltabuit G. & Vázquez G., 2007), hay que especificar el alcance de las políticas y los objetos de las mismas, consistentemente con la misión de seguridad previamente establecida.

Según Howard, (2003, p.13) “Política es la declaración de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboraron con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías.

Una política de seguridad en el ámbito de la criptografía de clave pública o PKI es un plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad. Pueden cubrir cualquier cosa desde buenas prácticas para la seguridad de un solo ordenador, reglas de una empresa o edificio, hasta las directrices de seguridad de un país entero.

Es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad

ISO 27002

Cuando se empieza a hablar sobre seguridad de la información nos viene a la mente la norma ISO 27001, esta norma es muy relevante ya que toma como base para todas las organizaciones a todos los riesgos que ésta se puede afrontar en su día a día, tiene como objetivo principal mantener, implantar, establecer y mejorar de forma continua la seguridad en las organizaciones. Sin embargo, otras normas también ocupan un papel que no debemos olvidarnos. En este caso la norma ISO 27002 del cual hablaremos y que se establece un catálogo lleno de buenas prácticas que determina toda la experiencia y una serie de objetivos de controles y que se integran en uno sólo todos los requisitos de la norma ISO 27001 con todo el tratamiento de los riesgos. Lo importante de disponer con una completa, actualizada y veraz información es

la clave para la realización de todas las actividades de una organización, en todos los ámbitos de sus campos, áreas y actividades. Sin embargo, es mucho más importante mantener toda la información con mucha seguridad para que no se pierda, la roben o se deteriore de alguna forma. Al final de todo, la información y los datos de los que cuenta la organización y que recolecta en su día a día son uno de los activos más importantes que puede marcar el futuro de la organización. Con ésta información es fácil decir y comprender la importancia de la norma ISO 27001 como Sistema de Gestión de Seguridad de la Información. Sin embargo, su papel es igual de importante que ocupa dentro de todos los requisitos de la norma ISO 27002 como una guía de buenas prácticas para implantar controles que garantizan la seguridad de la información gracias a sus recomendaciones. La norma ISO 27002 se encuentra estructurada en 14 capítulos que describen las áreas que se deben aplicar para garantizar la correcta seguridad de la información que se dispone. El documento recomienda total 114 controles, que no hace cumplirlos todos, pero si hay que tenerlos en cuenta y además del grado de la misma, considerar su posible aplicación.

Realizaremos **una revisión muy breve** de los 14 capítulos.

1. Políticas de Seguridad de la Información

En este capítulo se hace hincapié la importancia que ocupa la disposición de lo que es una adecuada política de seguridad, aprobada por la dirección y comunicada a todo el personal, siendo revisada de forma periódica y actualizada con los cambios que puedan producirse en el interior y exterior.

2. Organización de la Seguridad de la Información

Dentro de este capítulo los controles indicados buscan **estructurar un marco de seguridad** muy eficiente tanto mediante las tareas, seguridad, roles, etc. como en los celulares.

Es importante tener presente que cada vez es mayor el peso que ocupa el teletrabajo dentro de las empresas, es por ello, qie se deben tener en cuenta sus características especiales para que en ningún momento se ve afectada la seguridad de la información que se dispone.

3. Seguridad relativa a los recursos humanos

Podemos analizar de forma notable que los incidentes de seguridad que se producen en una organización, la gran mayoría de éstos tienen su origen de error humano. Es por ello que se debe concienciar y formar bien al personal de los términos de empleo de la información en el desarrollo de sus actividades y la importancia que tiene esa información en el desarrollo de sus actividades, además la importancia que tiene mantener, promover y mejorar el nivel de seguridad adecuándolo a las características de los datos y la información que se maneja es clave y gran parte de los objetivos que se debe perseguir.

4. Gestión de activos

Este capítulo se centra en la atención de los activos como información y en cómo deben ser las medidas para guardarlos y evitar tengan incidencias, quiebres en la seguridad y posiblemente una alteración no deseada.

5. Control de acceso

Control de acceso quiere decir quien accede a la información, dentro de un aspecto relevante. Al final de todo, no todas las personas de una organización necesitan tener accesos a todo para la realización de sus actividades diarias o a todos los datos, si no que tendremos personas que lleven roles que necesiten un acceso limitado como otras que necesitan un mayor acceso.

Para marcar las diferencias, se debe establecer todos los controles de los registros de los usuarios, gestión de privilegio de los accesos, etc. siendo algunos de los controles que se incluyen en este apartado.

6. Criptografía

En caso de que contemos con información sensible o crítica puede ser interesante utilizar muchas técnicas de criptología para proteger y garantizar su autenticidad, confidencialidad e integridad.

7. Seguridad física y del entorno

No se debe ver la seguridad solo a nivel técnico sino también físico, es decir, una labor tan simple como no dejar las pantallas e impresoras en zonas de fácil acceso, por parte del personal externo los documentos con los que están trabajando no sólo nos permitirá trabajar de forma adecuada la seguridad, si no que se acabarán convirtiendo en buenos ámbitos que nos aportan una buena eficiencia en la gestión.

8. Seguridad de las operaciones

Es un marcado componente técnico centrado en todos de disponibilidad como la protección de un software malicioso, control de software en exploración, copias de seguridad, gestion de vulnerabilidad, etc.

9. Seguridad de las comunicaciones

Las redes sociales son el medio por el cual se da la gran mayoría de los intercambios de información y de datos de distintas escalas, partiendo de ello, debemos garantizar la seguridad y proteger adecuadamente los medios de transmisión de éstos datos muy importantes.

10. Adquisiciones, desarrollo y mantenimiento de los sistemas de información

La seguridad de la información no es aspecto general de una sóla área, ni de un sólo proceso, no que es general, abarca a toda la organización y debe estar presente como un elemento transversal que es clave dentro del ciclo de vida que lleva un sistema de gestión.

11. Relación de proveedores

Si la organización establece relaciones con proveedores o terceros, se deben se establecer de todas maneras medidas de seguridad, también pueden ser recomendables e incluso muy necesario en ciertos casos.

12. Gestión de incidentes de seguridad de la información

Para los incidentes de seguridad primero debemos de hablar de controles de seguridad, no podemos avanzar nada sin ello. Ya que se debe estar preparados para cuando en cualquier momento estos incidentes ocurran, se pueda dar una respuesta rápida y eficiente siendo éstas las claves para lograr prevenirlos en caso ocurran en un futuro.

13. Aspectos de seguridad de la información para la gestión de la continuidad de negocio

Hasta que perdemos un dato importante no sabemos que lo necesitamos. Es por ello que sufrir una pérdida de información muy relevante y no lograr recuperarla de alguna manera puede llegar a poner en peligro la continuidad de la organización.

14. Cumplimiento

No debemos hablar de Seguridad de la información, sin hablar de normas, legislación y políticas aplicables que estén relacionadas con éste campo y con las que conviven las organizaciones. Es necesario tener presente que ocupan un enorme lugar en cualquier sistema de gestión y deben garantizar que están actualizados con los últimos cambios y que se cumplen, siendo esencial para al final no llevarnos sorpresas desagradables.

La norma ISO 27002 (anteriormente denominada ISO 17799)

Es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La versión más reciente de la norma ISO 27002:2013. La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad, integridad y disponibilidad. Para saber más sobre los demás dominios puede leer La norma ISO 27002 complemento para la ISO 27001.

La norma ISO 27002 se encuentra enfocada a todo tipo de empresas, independientemente del tamaño, tipo o naturaleza. La norma ISO 27002 se encuentra organizado en base a los 14 dominios, 35 objetivos de control y 114 controles. El documento denominado política es aquel que expresa una intención e instrucción general de la forma que ha sido expresada por la dirección de la empresa. El contenido de las políticas se basa en el contexto en el que opera una empresa y suele ser considerado en su redacción todos los fines y objetivos de la empresa, las estrategias adoptadas para conseguir sus objetivos, la estructura y los procesos utilizados por la empresa. Además, de los objetivos generales y específicos relacionados con el tema de la política y los requisitos de las políticas procedentes de niveles mucho más superiores y que se encuentran relacionadas.

ISO 27001

La norma ISO 27001, es un estándar reconocido a nivel internacional que muchas organizaciones utilizan para implementar su Sistema de Gestión de Seguridad de la Información.

Concretamente, también ayuda a gestionar la seguridad de la información de las organizaciones, no importa el tamaño que, de éstas o su carácter público o privado, dado que para todas estas metodologías ofrece lo necesario para implantar la seguridad en la gestión de la información. Muchos de los responsables de las organizaciones al momento de decidir si implantar o no en su organización un Sistema de Gestión de la Seguridad de la Información se preguntan si vale la pena hacerlo bajo la certificación de la ISO 20007. Ante la constante incertidumbre de varios, indicaremos algunos de los múltiples beneficios que se supone se deben implantar para las organizaciones un SGSI de acuerdo a la ISO 27001. Para brindar información acerca de lo que se supone se debe tener para una organización un SGSI de acuerdo a la ISO 27001 se recomendamos consultar la información del artículo ISO 27001. Aspectos organizativos para la Seguridad de la Información.”.

Beneficios de implantar un SGSI de acuerdo a ISO 27001

Como hemos mencionado más arriba, para las organizaciones la certificación bajo la norma ISO 27001 de su Sistema de gestión de Seguridad de la Información aporta:

- **Reduce el riesgo de que se produzcan pérdidas de información** en las organizaciones. Por pérdidas también entendemos robos y corrupciones en la manipulación de la misma.

- **Se hace una revisión continua de los riesgos** a los que están expuestos los clientes. Adicionalmente, se hacen controles de manera periódica.
- **Establece una metodología** gracias a la cual se puede gestionar la seguridad de la información de forma clara y concisa.
- **Implanta medidas de seguridad** para que los propios clientes puedan acceder a la información. Gracias a contar con dicho Sistema de Gestión, obliga a que se realicen auditorías externas de manera periódica y este hecho permite identificar las incidencias que pudiera haber en el Sistema de Gestión de Seguridad de la Información, fomentando de este modo la mejora continua en la organización.
- Contar un SGSI otorga a la organización una **garantía frente a clientes y socios estratégicos** ya que muestra a la misma como un organismo preocupado por la confidencialidad y seguridad de la información que es depositada en la misma.
- Permite a las organizaciones **continuar operando con normalidad** en caso de producirse problemas importantes.
- Se puede hacer una **integración conjunta con otros Sistemas de Gestión Normalizados** tales como ISO 9001, ISO 14001, OHSAS 18001, entre otras.
- Hace que la organización esté cumpliendo **con la legislación vigente** en materia de información personal y propiedad intelectual.
- La seguridad en la información que ofrece implantar un SGSI de acuerdo a ISO 27001 favorece una **reducción de los costes y un mejor funcionamiento de los procesos.**
- Se convierte en un **elemento favorable para la empresa frente a la competencia,** pues el contar con un SGSI le hace aumentar su imagen a nivel internacional.
- Contribuye al **incremento en la motivación del personal**, ya que se desempeñan en una organización comprometida con la seguridad de la información.

TIPOS DE REDES

Existen varios tipos de redes, los cuales se clasifican de acuerdo a su tamaño y distribución lógica. Existen multitud de clasificaciones de redes nosotros vamos a centrarnos en algunas de ellas así tenemos.

Clasificación según su tamaño.

PAN: Es la interconexión de varios servidores y periféricos. Su extensión está limitada físicamente a un entorno de 200 metros.

LAN: red de área local se conectan varios equipos con un alcance limitado por los cables o por la potencia de las antenas inalámbricas. Por ejemplo, la red del instituto

MAN: red área metropolitana. Red formada por un conjunto de redes LAN en las que se conectan equipos, por ejemplo, los de la junta de Extremadura

WAN red de área amplia interconectan equipos en un entorno muy amplio, como un país usando la red telefónica

Según el medio físico

Que utilicen para su conexión nos encontramos con diferentes tipos de redes en función del medio físico utilizado para transmitir la información así tenemos:

Redes alámbricas: que utilizan los cables que serán de pares trenzados y normalmente con conectores RJ45, así utilizaremos cables paralelos para conectar el ordenador al Switch y cables cruzados para conectar ordenadores entre sí

Redes inalámbricas: La conexión inalámbrica se realiza mediante las ondas electromagnéticas que se propagan entre una antena emisora y una

receptora. Para conectar un ordenador a una red wifi es necesario por tanto una antena receptora y el software adecuado.

Normalmente las redes suelen ser hibridas es decir redes lan que tienen conexión por cable, pero en las que alguno de sus nodos es un punto de acceso wireless que permite la conexión inalámbrica de otros dispositivos wifi. Existen diferentes tipos de antena wifi:

wireless PCI se conecta a la placa base y sale una antena por detrás del ordenador.

Wirelss USB se conecta por USB es similar a un pendrive

PCMCIA se conecta por una ranura de expansión de los portátiles

WirelessminiPCI. Integrada en placas de portátiles

Según Topología de la red:

- **Bus o lineal**: tiene un cable central con derivaciones.
- **Estrella:** todos los ordenadores están conectados a un concentrador o Hub central y no están conectados entre sí.
- **Anillo:** todos se conectan describiendo un anillo, la información llega a un ordenador si no la necesita la pasa al siguiente.
- **Malla:** cada ordenador está conectado al resto de los equipos con más de un cable

SEGURIDAD INFORMÁTICA

Para llegar a una correcta definición de seguridad informática se debe conocer primero los conceptos de informática y seguridad respectivamente:

- **Seguridad:**

La definición de seguridad trae consigo una ausencia de amenazas, situación que en el mundo contemporáneo es muy difícil de sostener, las sociedades actuales son sociedades de riesgo.

Para Barry, et al. (1998 cap. I) "La palabra seguridad se refiere a la ausencia de riesgos que va desde los amplios campos del análisis internacional, pasando por la seguridad nacional que el Estado considera vital defender, hasta su sentido más restringido refiriéndose a la seguridad del ser humano, en la salvaguarda de sus intereses fundamentales y de su propia vida"

Según Nambela (1996) dijo: seguridad es todo aquello que permite defenderse de una amenaza.
En conclusión seguridad es eliminar la incertidumbre ante lo que puede pasar, la seguridad total no existe, sólo existe una seguridad razonable.

REDES INALÁMBRICAS

Para Hernández (2007, p.3) Es un sistema de comunicación de datos inalámbrico frecuentemente utilizado como alternativa a las redes LAN cableadas o como extensión de estas. Este sistema utiliza ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado. De esta forma, se realiza la modulación donde la información viaja sobre las portadoras de radio hasta el receptor remoto. Gracias a que utiliza la tecnología de radiofrecuencia, ésta permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Este tipo de redes van

adquiriendo con el tiempo una mayor importancia permitiendo la transmisión en tiempo real.

Según Definición ABC, redes inalámbricas son una de las creaciones más importantes y significativas de los últimos tiempos ya que son las redes que permiten establecer comunicaciones a través de internet sin el uso de cables o limitaciones físicas que retengan un medio como una computadora a un espacio físico. Las redes inalámbricas son también conocidas popularmente con el nombre en inglés wifi, abreviación del concepto wide fidelity o fidelidad amplia en castellano.

Según Gómez, (Cap. I p.2) Una red inalámbrica de área local (Wireless LAN) es un sistema flexible de transmisión de datos implementados como una extensión, o como alternativa, de una red cableada. Utiliza tecnología de radio frecuencia, transmite y recibe datos utilizando como medio el aire, minimizando la necesidad de una conexión de cable, permitiendo la combinación conectividad y movilidad. Una red de computadoras local inalámbrica es un sistema de comunicación de datos que utiliza tecnología de radiofrecuencia. En esta red se transmite y recibe datos sobre aire, minimizando la necesidad de conexiones alambricas, es decir, combinan la conectividad de datos son la movilidad de usuarios.

Para Cabezas, (2010 Resum.) Las redes inalámbricas han provocado un gran impacto en todos los ámbitos sociales y económicos. Tanto la comunicación por voz como la transferencia de datos, han pasado de ser herramientas ancladas a un lugar y conectadas con cables a elementos que pueden ser transportados y utilizados mientras nos movemos, en cualquier momento y en cualquier lugar. Por tanto, se han convertido en dispositivos con

tecnologías que permiten realizar actividades que antes solo podíamos desarrollar sentados en la oficina de una empresa, en el hogar o en un centro de investigación.

SEGURIDAD EN REDES INALÁMBRICAS

En los últimos años las redes de área local inalámbricas (WLAN, Wireless Local Area Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

La seguridad es una de los temas más importantes cuando se habla de redes inalámbricas.

Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito. Por ello es conveniente el seguir puntual y escrupulosamente una serie de pasos que nos permitan disponer del grado máximo de seguridad del que seamos capaces de asegurar.

Para Bustamante (2006, p. 2) La definición y el objetivo de la seguridad en redes es mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales) control y autenticidad de la información manejada por computadora, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo acuerdo.

GESTION DE INCIDENCIAS

La gestión de incidentes es un área de procesos perteneciente a la gestión de servicios de tecnologías de la información. El primer objetivo de la gestión de incidentes es recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo lo posible el impacto negativo en la organización de forma que la calidad del servicio y la disponibilidad se mantengan.

Una incidencia es toda interrupción o reducción de la calidad no planificada del servicio. Pueden ser fallos o consultas reportadas por los usuarios, el equipo del servicio o por alguna herramienta de monitorización de eventos.

3 conceptos básicos sobre la Gestión de Incidencias

Escala de tiempos

A partir del SLA se establecen los tiempos máximos en los que se deben responder y resolver las incidencias.

Debemos usar herramientas de gestión para el cálculo y la asignación de estas escalas de tiempo, así como para utilizar alertas y escalados para facilitar la respuesta/resolución de las incidencias dentro del tiempo máximo definido.

Modelos de incidencia

Los modelos de incidencia permiten optimizar el proceso de resolución.

Existen incidencias que no son nuevas, sino que ya se han producido anteriormente y que se volverán a producir en el futuro. Muchas empresas encuentran útil la definición de modelos de incidencia que se puedan aplicar a incidencias recurrentes del servicio.

- ✓ Un modelo de incidencia debería incluir:
- ✓ Los pasos a seguir para la resolución de la incidencia.
- ✓ El orden cronológico de estos pasos y sus dependencias si las hubiera.
- ✓ Responsabilidades: quién debe hacer qué.
- ✓ Plazos para la realización de las actividades.
- ✓ Procedimientos de escalado: quién debería ser contactado y cuando.

Incidencias graves

Cada servicio debe definir cuáles son los criterios para que una incidencia se considere grave.

Las incidencias graves deben tener asociado su propio procedimiento de resolución y escalado, y tener una escala de tiempos menor que el resto. La actividad de priorización, que veremos más adelante, debe tener en cuenta estos criterios.

ACTIVIDADES PRINCIPALES DE LA GESTIÓN DE INCIDENCIAS

- **Detección**

  Cuanto antes se detecte una incidencia, menor será su impacto en el negocio. Por lo tanto, es importante monitorizar los recursos con el objetivo de detectar incidencias potenciales y normalizar el servicio antes de que se produzca un impacto negativo en los procesos de negocio o, si esto no es posible, que el impacto sea mínimo.

- **Registro**

  Todas las incidencias del servicio deben ser registradas, y cada incidencia debe registrarse de forma independiente.
  La información a registrar generalmente incluye:

  – Identificador único.
  – Categorización.
  – Urgencia, impacto y prioridad.
  – Fecha y hora.
  – Persona/grupo que registra la incidencia.
  – Canal de entrada.
  – Datos del usuario.
  – Síntomas.
  – Estado.
  – CIs (Configuration Items, elementos de configuración) asociados.
  – Persona/grupo asignado para la resolución.
  – Problema/Known error asociado.
  – Actividades realizadas para la resolución.
  – Fecha y hora de la resolución.
  – Categoría del cierre.
  – Fecha y hora de cierre.

- **Categorización**

  En esta actividad se establece el tipo exacto de la incidencia.

  Generalmente se establece una categorización multinivel con dependencias entre niveles. El número de niveles dependerá de la granularidad con la que necesitemos tipificar las incidencias.

- **Priorización**

  Generalmente, la prioridad de la incidencia nos indica cómo se ha de gestionar.

  La prioridad de la incidencia suele depender de:

  – La urgencia: rapidez con que la incidencia necesita ser resuelta.

  – El impacto: generalmente se determina por el número de usuarios afectados, aunque lo realmente importante es la criticidad para el negocio de los usuarios afectados por la incidencia. Al final, lo que realmente determina el impacto son los aspectos adversos que la incidencia tiene en el negocio.

  Además de la urgencia y el impacto, la prioridad también puede depender de otros factores como si el usuario es VIP, el departamento del usuario, etc.

  Es muy conveniente que la herramienta de soporte utilizada sea capaz de **calcular la prioridad en base a reglas**. En cualquier caso, el equipo de soporte debe conocer estas reglas para poder priorizar adecuadamente.

- **Diagnóstico inicial**

  Cuando el personal de soporte de primer nivel recibe una incidencia, la diagnostica en base a los síntomas y, si está capacitado para ello, la resuelve.

- **Escalado**

  Existen dos tipos de escalado:

  1. Funcional: el soporte de primer nivel se ve incapaz de resolver la incidencia y la asigna al grupo resolutor correspondiente.

  2. Jerárquico: en caso de que se den ciertas circunstancias (incidencias graves o críticas, riesgo de incumplimiento del SLA) que se deban notificar a los responsables del servicio correspondiente.

  A pesar de que se produzca un escalado, la incidencia sigue perteneciendo al equipo de Service Desk, y es éste es el responsable de hacer el seguimiento de la misma y mantener informados a los usuarios hasta su cierre.

- **Investigación y diagnóstico**

  Si la incidencia hace referencia a un fallo en el sistema, lo más probable es que se necesite investigar la causa del fallo.

  Las tareas más comunes dentro de esta actividad son las siguientes:

Establecer exactamente **qué es lo que no funciona** correctamente y para qué secuencia de acciones del usuario (casuística).

Establecer el **impacto** potencial de la incidencia.

Determinar si la incidencia está producida por la implantación de **un cambio.**

Buscar en la **base de datos de conocimiento** (base de datos de errores conocidos, registro de incidencias, etc.) posibles soluciones y/o workarounds.

- **Resolución**

Cuando se detecta una solución potencial, ésta debería ser aplicada y testeada. Una vez comprobada la resolución, la incidencia se da por resuelta y se asigna al equipo de Service Desk para su cierre.

Asimismo, **se deben registrar todas las acciones** realizadas para resolver la incidencia en el historial de la misma.

- **Cierre**

Antes de cerrar la incidencia el equipo del Service Desk debería validar lo siguiente:

- ✓ Si el usuario está satisfecho con la resolución de la incidencia.
- ✓ Si el cierre ha sido categorizado.
- ✓ Si se han cumplimentado todos los datos necesarios.

- ✓ Si es un problema recurrente. En este caso, generar un problema.

- ✓ Eventualmente, se puede pasar una encuesta de satisfacción al usuario.

¿Por qué Gestión de Incidencias?

Toda empresa de servicios necesita la Gestión de Incidencias para prevenir o restaurar tan pronto como sea posible cualquier interrupción o reducción no planificada en la calidad de su servicio.

Sin embargo, debemos ser conscientes de los desafíos y riesgos de la Gestión de Incidencias con el fin de garantizar la mejor operación de servicio.

2.3. Definición de términos

WNCOR: Es el nombre de la red inalámbrica de IBK por el cual se puede conectar cualquier usuario del banco o proveedor siempre y cuando el equipo se encuentre dentro del dominio del banco. En ella se tiene todos los accesos de la misma manera que te puede tener con un cable de red, la wncor es utilizada en todas las sedes de IBK mas no en las tiendas del Banco

IBK: Es el abreviado de Interbank.

TIENDAS: tiendas son llamadas los bancos de atención al público en otras palabras las tiendas son las agencias bancarias, ellas están enumeradas por números de esa forma y con un nombre estas pueden ser identificadas. Ejemplo: Interbank – Tienda 500 MM Huancayo.

CDS: Centro de Servicios, es la mesa de ayuda al cual el usuario llama para recibir un primero apoyo al cual también le llamamos el primer Nivel y el Segundo Nivel es el área técnica, todos ellos se encuentran en el grupo del Centro de Servicios.

IMAC: Un IMAC es una denominación que se le da al ticket generado al momento que el usuario requiere una atención técnica, a diferencia de los otros tickets estos son generados como requerimientos y no como incidencias ya que conlleva a un cobro adicional fuera del contrato que tiene Sapia con IBK y este cobro es cargado al Centro de costos del usuario que tiene dentro de su área.

SGSI: Sistemas de Gestión de Seguridad de la Información

ISO: International Organization for Standardization (Organización Internacional de Normalización)

AD: Active Directory, es el sistema donde se visualizan todos los accesos que los usuarios cuentan de la organización.

ISO 27001: Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

2.4. HIPÓTESIS

2.4.1. Hipótesis General

- La Implementación un modelo de buenas prácticas aplicando ISO 27002 mejorará la gestión de incidencias de la red Wncor.

2.4.2. Hipótesis Específicas

a) El modelo de buenas prácticas aplicando ISO 27002 reducirán los problemas de conexión de la red Wncor.

b) El modelo de buenas prácticas aplicando ISO 27002 reducirá los problemas de ingreso a los file server de la red Wncor.

2.5. VARIABLES

2.5.1. Definición conceptual de la variable

Variable Independiente (VI): Modelo de buenas prácticas aplicando la Norma ISO 27002. La Norma a utilizar un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. Ésta variable nos ayudará según el procesamiento de datos a saber cuáles de sus 114 controles elegir para aplicarlas en la mejoría y reducción de incidencias en la red Wncor. La versión más reciente de la norma ISO 27002:2013. La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad, integridad y disponibilidad. Para saber más sobre los demás dominios puede también se tiene La norma ISO 27002 complemento para la ISO 27001.

Variable Dependiente (VD): Gestión de incidencias de la red Wncor. La gestión de incidencias es un área de procesos perteneciente a la gestión de servicios de tecnologías de la información. El primer objetivo de la gestión de incidentes es recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo lo posible el impacto negativo en la organización de forma que la calidad del servicio y la disponibilidad se mantengan. El resultado de nuestra variable dependerá de la aplicación que se haga de nuestra variable independiente, siguiendo los pasos también que la gestión de incidencias nos brinda para resolver los problemas de conexión a la red Wncor.

2.5.2. Definición operacional de la variable

Problemas de conexión: Los usuarios de IBK se conectan de forma inalámbrica a la red Wncor ya que de esa manera les permite desplazarse a cualquier piso de la sede sin perder la conectividad y estar dentro del dominio. Pero muchas de las incidencias se producen median la Wncor. Si bien los usuarios ya estuvieron conectados un día anterior al siguiente día tienen problemas al querer conectarse sin poder acceder a la Wncor.

Incidencias con File Server: Los archivos en toda organización son importantes y en IBK se tiene la facilidad de ingresar a archivos mediante servidores compartidos (File Servers) en los cuales para contar con esos archivos primeros los usuarios deben solicitar el acceso y una vez que cuentan pueden tener el libre ingreso. Pero las incidencias en los file server son continuos ya que aun teniendo el acceso los usuarios muchas veces no pueden ingresar estando conectados en la Wncor, a pesar de que el día anterior si lograron ingresar al siguiente ya no es posible. Otras de las incidencias también es que no logran pegar archivos en el file server a pesar de tener accesos de lectura y escritura.

2.5.3. Operacionalización de la variable

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADOR
MODELO DE BUENAS PRÁCTICAS	Un modelo de buenas prácticas son iniciativas, medidas y políticas que una empresa establece para mejorar la calidad de la vida laboral de sus empleados. Lo importante de estas iniciativas es que van más allá de lo que la legislación laboral establece, es decir no son obligatorias.	Se centra en las buenas prácticas para gestión de la seguridad de la información, es fundamental para la consolidación de un SGSI garantizando la continuidad y el mantenimiento de los procesos de seguridad, alineados a los objetivos estratégicos de la organización.		
GESTION DE INCIDENCIAS	La gestión de incidentes es un área de procesos perteneciente a la gestión de servicios de tecnologías de la información. El primer objetivo de la gestión de incidentes es recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo lo posible el impacto negativo en la organización de forma que la calidad del servicio y la disponibilidad se mantengan.	Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio. El objetivo es reiniciar el funcionamiento normal tan rápido como sea posible con el menor impacto para el negocio y el usuario con el menor coste posible.	Confidencialidad Responsabilidad Compromiso Accesibilidad	- Fallos de conexión a red Wncor. - Fallos de ingreso a file server.

CAPITULO III
METODOLOGÍA

3.1. Método de investigación

INVESTIGACIÓN CIENTÍFICA

Para esta investigación se utilizará la **investigación científica** por que aplicamos todo un proceso de Investigación para descubrir y obtener información relevante, ésta posee una serie de pasos para lograr el objetivo planteado o para llegar a la información solicitada

Además, la investigación posee una serie de características que ayudan al investigador a regirse de manera eficaz en la misma, es tan compacta que posee formas, elementos, procesos, diferentes tipos, entre otros. El método científico indica el camino que se ha de transitar en esa indagación y las técnicas precisan la manera de recorrerlo.

3.2. Tipo de investigación

INVESTIGACIÓN APLICADA

El tipo de investigación que se persigue en la investigación es aplicada. Vélez S. (2001), afirma “Persigue fines inmediatos y concretos, a través de la búsqueda de la obtención de un nuevo conocimiento técnico con aplicación inmediata a un problema determinado”. Nos es útil porque se resuelve el problema enfocándonos en la aplicación de las buenas prácticas que la Norma ISO 27002 nos brinda y ello nos ayuda con la gestión de las incidencias que los usuarios de Interbank reportan a diario. Además, las buenas prácticas fueron aplicadas en los mismos usuarios de Interbank obteniendo buenos resultados.

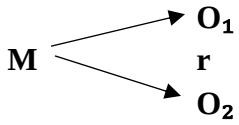
3.3. Nivel de Investigación

INVESTIGACION CORRELACIONAL

La investigación correlacional es un tipo de método de investigación en el cual un investigador mide dos variables. Entiende y evalúa la relación estadística entre ellas sin influencia de ninguna variable extraña.

Pues en esta investigación se correlacionan las dimensiones de los indicadores para elegir las políticas correctas de la ISO 27002 y aplicarlas en los usuarios de Interbank, con esto se ven los resultados de causa y efecto entre las dos variables (Variable Independiente y Variable Dependiente).

Esto es precisamente lo que es la investigación correlacional, hacer una relación entre dos variables. La investigación correlacional busca variables que parecen interactuar entre sí, de modo que cuando una variable cambia, la persona, al hacer una investigación, tendrá clara la manera en la que la otra variable también cambia.



Donde:
M = Muestra.
O_1 = Variable 1
O_2 = Variable 2.
r = Relación de las variables de estudio.

3.4. Diseño de investigación

INVESTIGACION PRE EXPERIMENTAL

> Presentan el más bajo control de variables y no efectúan asignación aleatoria de los sujetos al experimento, y son aquellos en los que el investigador no ejerce ningún control sobre las variables extrañas o intervinientes, no hay asignación aleatoria de los sujetos participantes de la investigación ni hay grupo control (2010, p.146.)

Con los conceptos obtenidos, para el desarrollo de ésta tesis se utilizará la investigación experimental debido a que se tuvo que manipular las variables, realizando antes una previa evaluación a nuestra investigación y luego otra prueba después de la aplicación de la Norma ISO 27002 para comparar los resultados y puedan ser demostrados en las Hipótesis.

3.5. Población y muestra

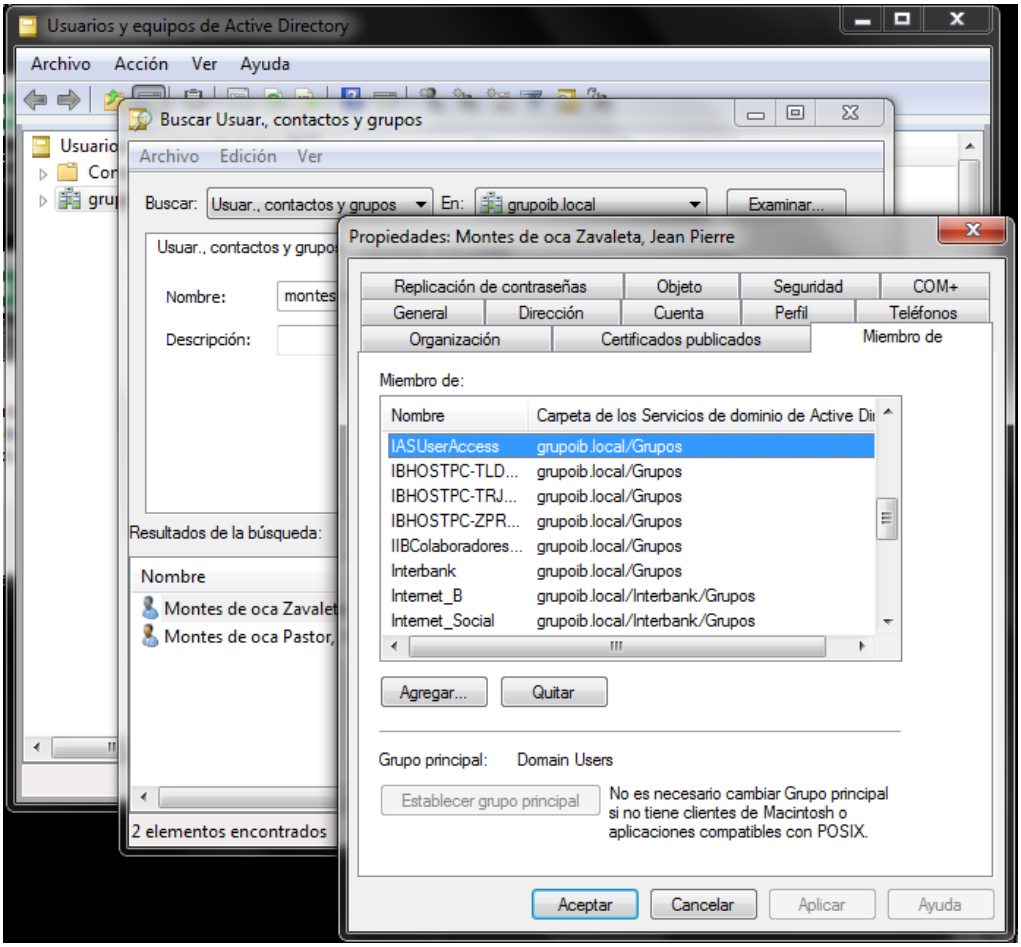
POBLACION

La población a utilizar serán los usuarios de Interbank alojados en la sede Torre Interbank, ubicados en Carlos Villarán 140, La Victoria 15034, que son aproximadamente 1000 trabajadores seleccionando del sistema sólo a los usuarios que cuentan con accesos a la Red Wncor, el cual podemos darnos cuenta que cuentan con los accesos si pertenecen al grupo IASUSER en el **AD (Active Directory)** Sistema en el cual se muestran todos los accesos que los usuarios cuentan.

Hurtado (2000), la población se define “como el conjunto de elementos, seres o eventos concordantes entre sí en cuanto a una serie de características, de la cuales se desea obtener alguna información”

Para Chávez (2007) la población de un estudio se define como “el universo de la investigación sobre el cual se pretende generalizar los resultados”.

Por otra parte, de acuerdo a Hernández y Baptista (2003) la población es el conjunto de todos los casos que concuerdan con una serie de especificaciones, que pueden ser estudiados y sobre los que se pretende generalizar los resultados.



Una vez que se obtuvo la información de los usuarios que cuentan con accesos a la red Wncor se procedió con la participación de las encuestas de forma aleatoria, asegurando así que el proyecto se trabajó sólo con los usuarios apropiados.

MUESTRA

Sabino (1992), la define como la "parte del todo que llamamos universo y que sirve para representarlo". Tiene diferentes definiciones según el tipo de estudio que se esté realizando. Para los estudios cuantitativos, no es más que un "subgrupo de la población del cual se recolectan los datos y debe ser representativo de dicha población"

La cantidad de trabajadores de la Sede Interbank es de 1000 usuarios aproximadamente, de los cuales se verificó con el Sistema Active Directory que 500 usuarios cuentan con accesos a la red Wncor.

Dado que se conoce el tamaño de la población total de usuarios de la Torre de Interbank que cuentan con accesos a la Red Wncor y que cada uno de ellos pertenece al grupo IASUSER registrado en el Active Directory, el cálculo de la muestra se realizará de la siguiente manera.

$$n = \frac{Z^2 pqN}{NE^2 + Z^2 pq}$$

Donde:

n: tamaño de muestra aproximado

N: tamaño total de la población que se está utilizando. (N=500)

Z: Nivel de confianza. (Z= 1.96) que corresponde al 95% de confianza según la tabla de distribución normal.

E: Margen de error. (E=0.15)

p=q: Probabilidad de éxito y fracaso (0.5)

$$n = \frac{(1.96)^2\,(0.5)\,(0.5)\,(500)}{(500)(0.15)^2 + (1.96)^2(0.5)\,(0.5)}$$

$$\mathbf{n = 39.33}$$

Por lo tanto, el tamaño de la muestra es de 40 usuarios, todos cuentan con el acceso y son afectados con las incidencias de la Red Wncor.

Se entiende por muestra al "subconjunto representativo y finito que se extrae de la población accesible" (Ob. cit. p. 83). Entonces según lo afirmado por el autor, en la presente investigación se utilizará el tipo de **Muestreo Probabilístico**

MUESTREO PROBABILISTICO

Lo llamamos muestreo probabilístico porque se utilizó una muestra pequeña pero muy probable para obtener los resultados ya que todas las encuestas fueron aplicadas netamente a los usuarios que cuentan con los accesos a la Red Wncor, asegurando así que sus respuestas son claras y precisas, por lo que se realizaron preguntas que se acomodan a las molestias que éstos usuarios tenían y que se quisieron resolver.

3.6. Técnicas e instrumentos de recolección de datos

Hernández, et al., (2003), sugieren que éstos son un “recurso que utiliza el investigador para registrar informaciones o datos sobre las variables que tiene en mente”, (p.346).

En esta etapa de la investigación se definen los medios y recursos utilizados para recabar la información bien sea la observación directa de documentales y entrevistas.

Así mismo, sobre el mismo aspecto, Avilez (2007) se refiere a las técnicas de recolección de datos, como el uso de una diversidad de técnicas y herramientas que pueden ser utilizadas por el analista con el fin de desarrollar los sistemas de información. Ejemplo la entrevista, la encuesta, el cuestionario, la observación, el diagrama de flujo y el diccionario de datos, entre otros.

Según Méndez (2001) la observación directa, identificada como; el proceso mediante el cual se perciben deliberadamente ciertos rasgos existentes en la realidad por medio de un esquema conceptual previo y con base en ciertos propósitos definidos generalmente por una conjetura que se quiere investigar.

Otra significativa y valiosa técnica es las encuestas; definida por Tamayo Tamayo (2007) como una "técnica o procedimiento que recoge información directa o indirecta formulando preguntas, las cuales son formadas y llenadas por un empadronador frente a quien le responde".

Encuesta. Según afirma Avila Baray (2006), la encuesta "se utiliza para estudiar poblaciones mediante el análisis de muestras representativas a fin de explicar las variables de estudio y su frecuencia.

INSTRUMENTOS

Cuestionarios: Los cuestionarios serán entregados a los usuarios de IBK que se basará en preguntas que nos ayudarán a consultar que tan seguidos son sus incidencias con la red Wncor y descubrir que el uso que le dan, con ello sabremos un poco más de las malas prácticas que aplican en la red.

Ficha de registro: Los reportes de las incidencias serán sacados del sistema CA Service Desk que es el sistema de registro de tickets que se generan por cada incidencia que presentan los usuarios y son guardados por defecto con datos como: Fecha de apertura, fecha de solución, descripción breve del

problema, descartes realizados, usuario afectado, grupo que solucionó el incidente. Con estos datos podremos sacar la información de cantidad de usuarios afectados por el periodo de tiempo que necesitemos.

3.7. Procesamiento de información

SPSS

Es un programa estadístico informático muy usado en las ciencias sociales y aplicadas, además de las empresas de investigación de mercado. El nombre originario correspondía al acrónimo de Statistical Package for the Social Sciences (SPSS), reflejando la orientación a su mercado original (ciencias sociales), aunque este programa es también muy utilizado en otros campos como la mercadotecnia. Sin embargo, en la actualidad la parte SPSS del nombre completo del software (IBM SPSS) no es acrónimo de nada.

Es uno de los programas estadísticos más conocidos teniendo en cuenta su capacidad para trabajar con grandes bases de datos y una sencilla interfaz para la mayoría de los análisis. En la versión 12 de SPSS se podían realizar análisis con dos millones de registros y 250.000 variables. El programa consiste en un módulo de base y módulos anexos que se han ido actualizando constantemente con nuevos procedimientos estadísticos. Cada uno de estos módulos se compra por separado. Por ejemplo, SPSS puede ser utilizado para evaluar cuestiones educativas. Actualmente, compite no sólo con programas licenciados como SAS, MATLAB, Statistica, Stata, sino también con software de código abierto y libre, de los cuales el más destacado es el Lenguaje R. Recientemente ha sido desarrollado un paquete libre llamado PSPP, con una interfaz llamada PSPPire que ha sido compilada para diversos sistemas operativos como Linux, además de versiones para Windows y macOS. Este último paquete pretende ser un clon de código abierto que emule todas las posibilidades del SPSS.

3.8. Técnicas y análisis de datos

Sabino (1992), afirma que este aspecto de las investigaciones no es más que la "implementación instrumental del diseño escogido"

Por procedimiento de procesamiento en la investigación, debe entenderse el conjunto de métodos y técnicas que se emplean en la tabulación medición y síntesis de los datos.

PRUEBA DE CHI-CUADRADO

El procedimiento Prueba de chi-cuadrado tabula una variable en categorías y calcula un estadístico de chi-cuadrado. Esta prueba de bondad de ajuste compara las frecuencias observadas y esperadas en cada categoría para contrastar que todas las categorías contengan la misma proporción de valores o que cada categoría contenga una proporción de valores especificada por el usuario.

La prueba de chi o Ji cuadrado (X2), es sin duda la más conocida y probablemente la más utilizada para el análisis de variables cualitativas. Su nombre lo toma de la distribución Chi cuadrado de la probabilidad, en la que se basa. La prueba de chi cuadrado de independencia entre dos variables cualitativas fue desarrollada ya en 1900 por Pearson, y su utilidad es precisamente evaluar la independencia entre dos variables nominales u ordinales, dando un método para verificar si las frecuencias observadas en cada categoría son compatibles con la independencia entre ambas variables. Para evaluarla se calculan los valores que indicarían la independencia absoluta, lo que se denomina frecuencias esperadas, comparándolos con las frecuencias de la muestra.

ALFA DE CRONBACH

El Alfa de Cronbach es un coeficiente que sirve para medir la fiabilidad de una escala de medida, y cuya denominación Alfa fue realizada por Cronbach en 1951. Un investigador trata de medir una cualidad no directamente observable (por ejemplo, la inteligencia) en una población de sujetos. Para ello mide n variables que sí son observables (por ejemplo, n respuestas a un cuestionario o un conjunto de n problemas lógicos) de cada uno de los sujetos.

COEFICIENTE DE CORRELACIÓN DE SPEARMAN

En estadística, el **coeficiente de correlación de Spearman**, ρ (rho) es una medida de la correlación (la asociación o interdependencia) entre dos variables aleatorias (tanto continuas como discretas). Para calcular ρ, los datos son ordenados y reemplazados por su respectivo orden.

PRUEBA DE LOS RANGOS CON SIGNO DE WILCOXON

La prueba de los rangos con signo de Wilcoxon es una prueba no paramétrica para comparar el rango medio de dos muestras relacionadas y determinar si existen diferencias entre ellas. Se utiliza como alternativa a la prueba t de Student cuando no se puede suponer la normalidad de dichas muestras.

CAPITULO IV:
RESULTADOS

Análisis actual de sucesos aplicados por usuarios de Interbank

A continuación, se muestra en interpretación gráfica el resultado de la encuesta aplicada a los usuarios de Interbank, en el que verificaremos el estado inicial de las malas prácticas que interactuaban los usuarios diariamente con respecto a la red Wncor. Este resultado tuvo como finalidad recolectar datos que fueron utilizados para la investigación.

Se representará en cada tabla cada una de las preguntas que fueron cuestionadas a los usuarios de Interbank, para obtener un resultado completo con datos de frecuencia, porcentaje, porcentaje válido y porcentaje acumulado, además de mostrarse en gráficos una mejor demostración de los resultados para lograr entenderlos fácilmente.

Se describen también de que manera afectan estas malas prácticas en las incidencias que se presentan por conexión a la Red Wncor y Fallos de ingresos a File Server, cuál es su motivo y el error que ocasionan tanto para las incidencias investigadas como para las demás incidencias que se presentan a nivel general.

Indica también alguno de los motivos que los usuarios optan por realizar estas malas prácticas, ya sea por facilidad, rapidez, comodidad, o desconocimiento pero que hacen que el resultado final sea tener las incidencias ya descritas.

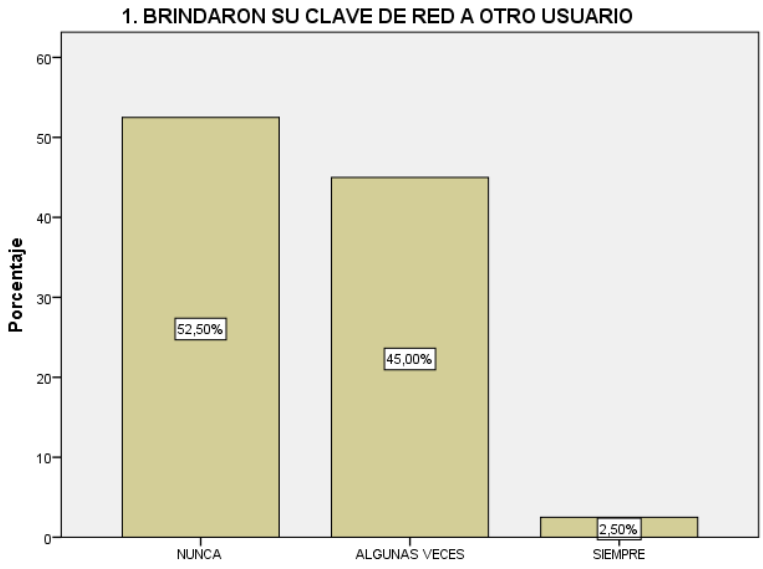
PREGUNTA1: ***¿Alguna vez has brindado tu clave de red a otro usuario?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que brindaban su clave de red a otros usuarios antes de aplicarse la *NTP ISO/IEC 27002.*

Tabla 1: Medidas descriptivas de usuarios que brindan su clave de red

1. BRINDARON SU CLAVE DE RED A OTRO USUARIO

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	21	52,5	52,5	52,5
	ALGUNAS VECES	18	45,0	45,0	97,5
	SIEMPRE	1	2,5	2,5	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 1: Porcentaje de usuarios que brindan su clave de red.

Ésta mala actividad es una de las principales causas de incidencia para el ingreso a la red Wncor, ya que al brindar su clave de red a otros usuarios corren el riesgo que éstos no la recuerden bien al ingresarlo y la cambien, pues al cambiarlo y no cerrar sesión o reiniciar el equipo, el sistema desactiva todos los accesos para la Wncor y para las demás aplicaciones y entre ello complicar el ingreso al File Server.

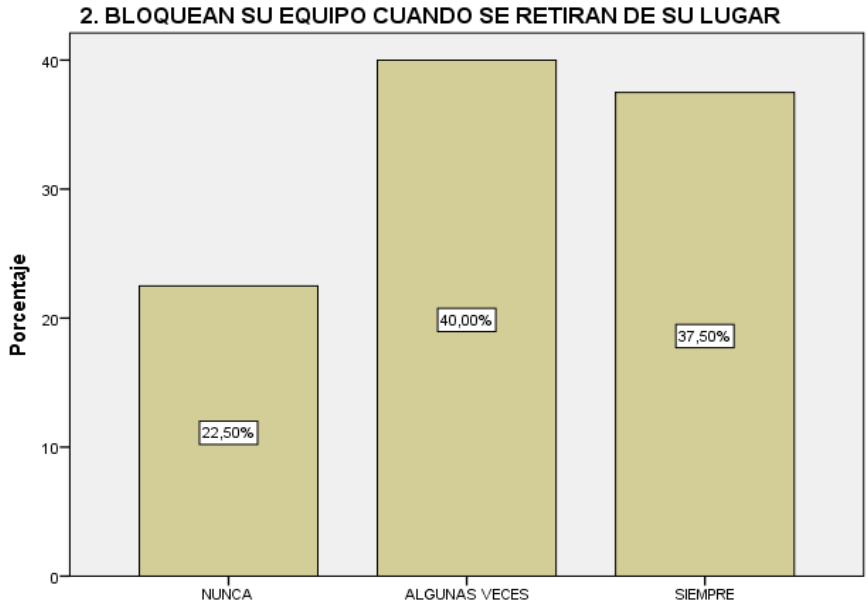
PREGUNTA2: ***¿Bloqueas tu pc cuando sales de tu lugar?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que bloqueaban su equipo cuando se retiran de su ubicación antes de aplicarse la NTP ISO/IEC 27002.

Tabla 2: Medidas descriptivas de usuarios que bloquean su equipo cuando se retiran de su lugar.

2. BLOQUEAN SU EQUIPO CUANDO SE RETIRAN DE SU LUGAR

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	9	22,5	22,5	22,5
	ALGUNAS VECES	16	40,0	40,0	62,5
	SIEMPRE	15	37,5	37,5	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 2: Porcentaje de usuarios que bloquean su equipo cuando se retiran de su lugar.

Ésta pregunta también fue cuestionada para saber el nivel de riesgo que los usuarios exponen a Interbank, pues al no bloquear su equipo al retirarse de su ubicación exponen a que cualquier otro usuario que sepa su contraseña de red puede ingresar, robar información, manipular la red o cambiar la contraseña complicando así la conexión al siguiente inicio de sesión a la Red Wncor y en caso no sea reiniciado la PC o cerrado sesión traer problemas.

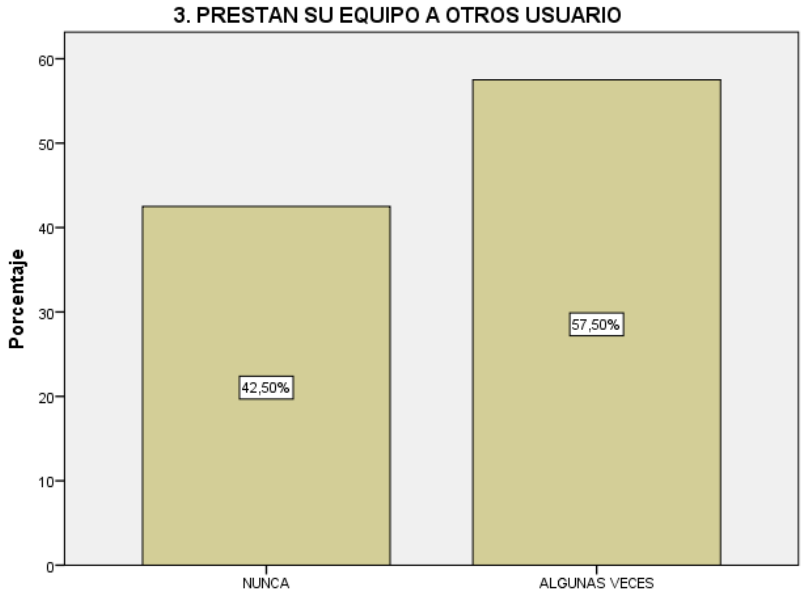
PREGUNTA 3: ***¿Prestaste tu equipo a otro usuario?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que prestaron sus equipos a otros usuarios antes de aplicarse la *NTP ISO/IEC 27002.*

Tabla 3: Medidas descriptivas de usuarios que prestan su equipo a otros usuarios.

3. PRESTAN SU EQUIPO A OTROS USUARIO

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	17	42,5	42,5	42,5
	ALGUNAS VECES	23	57,5	57,5	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 3: Porcentaje de usuarios que prestaron su equipo a otros usuarios.

Existen en Interbank muchos usuarios que utilizan laptops, PC's, Tablets, etc. por lo que este proyecto está aplicado sólo para usuarios que lo utilizan laptops o equipos portátiles. La pregunta fue aplicada para identificar la cantidad de usuarios que aplican ésta mala práctica pues al hacerlo, los usuarios a quienes fueron prestado los equipos manipulan la laptop des configurando en muchas ocasiones lo que ya está configurado sólo para el usuario principal, pues ingresan otra clave de red, inician otra sesión, instalan otros aplicativos, cambian el nombre del equipo sin que después haya sido informado al usuario principal y después éste tenga problemas para el ingreso a la red Wncor y al ingreso de sus File Server.

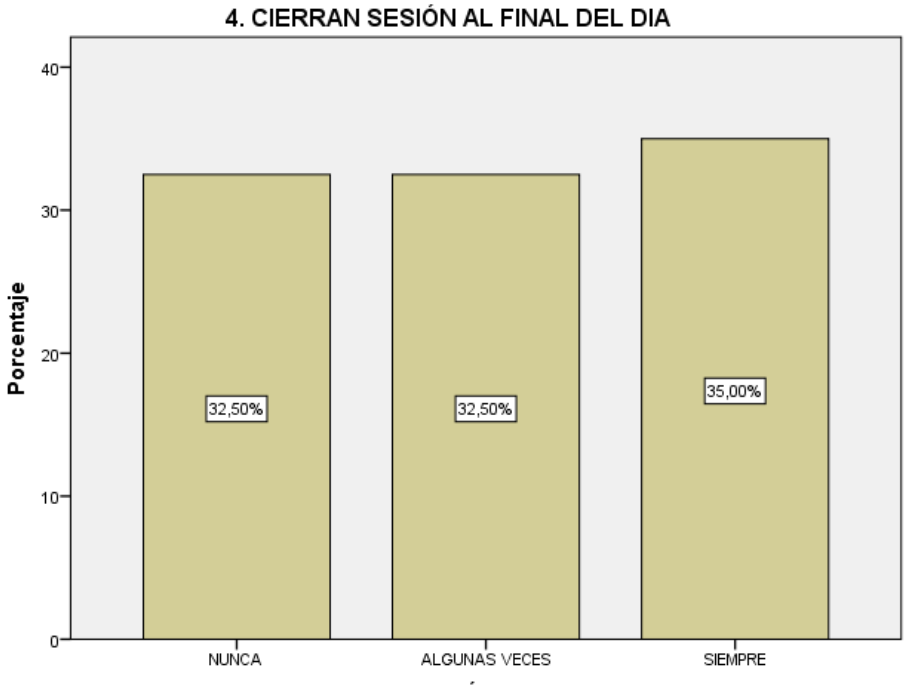
PREGUNTA 4: ***¿Cierras la sesión de tu equipo al final del día?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que cierran su sesión al final del día antes de aplicarse la *NTP ISO/IEC 27002.*

Tabla 4: Medidas descriptivas de usuarios que cierran sesión al final del día.

4. CIERRAN SESIÓN AL FINAL DEL DIA

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	13	32,5	32,5	32,5
	ALGUNAS VECES	13	32,5	32,5	65,0
	SIEMPRE	14	35,0	35,0	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 4: Porcentaje de usuarios que cierran sesión al final del día.

Los usuarios de IBK tienen sus propias terminales, cada equipo está asignado a cada usuario con un nombre de Equipo, entonces, si los usuarios no cierran sesión de su PC y otro usuario sabe el nombre de su equipo que es una nomenclatura igual para todos y fácil de adivinar es muy probable que cualquier otro usuario ingrese a su sesión si ésta no ha sido cerrada, poniendo así en riesgo a la perdida y/o robo de información. Es por ello que se consideró esta pregunta para identificar la cantidad de usuarios que no realizan el cierre de su Sesión.

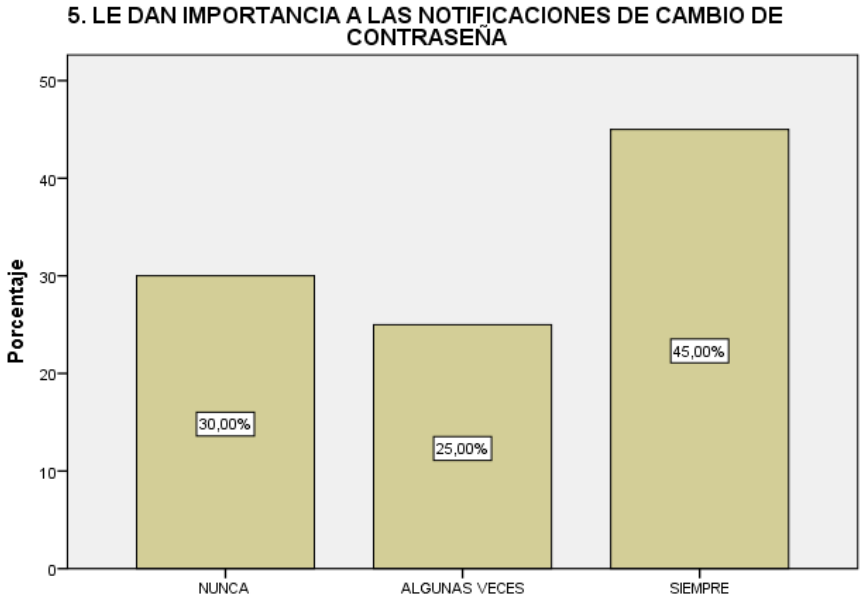
PREGUNTA 5: ***¿Le das importancia a las notificaciones de cambio de contraseña?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que le dan importancia a las notificaciones antes de aplicarse la *NTP ISO/IEC 27002*.

Tabla 5: Medidas descriptivas de usuarios que le dan importancia a las notificaciones de cambio contraseña.

5. LE DAN IMPORTANCIA A LAS NOTIFICACIONES DE CAMBIO DE CONTRASEÑA

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	12	30,0	30,0	30,0
	ALGUNAS VECES	10	25,0	25,0	55,0
	SIEMPRE	18	45,0	45,0	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 5: Porcentaje de usuarios que le dan importancia a las notificaciones de cambio contraseña.

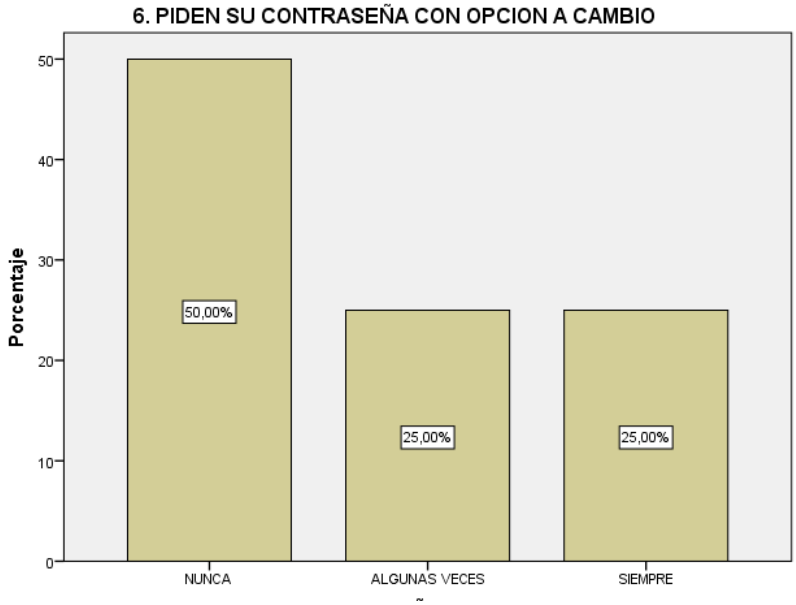
Se muestran usuarios que algunas veces y nunca les dan importancia a las notificaciones de cambio de contraseña, esto representa un alto desinterés de los usuarios ya que si la contraseña no es cambiada antes de la fecha de caducidad no es posible el ingreso a la sesión, a la Wncor como a ningún otro aplicativo incluyendo a los File Server, ya que la clave de red es la clave principal para el inicio en el sistema y esta debe ser aceptada correctamente para no tener incidencias.

PREGUNTA 6: ***¿Pides tú contraseña con opción a cambio al Centro De Servicios?***
Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios piden su contraseña con opción a cambio al Centro de Servicios antes de aplicarse la *NTP ISO/IEC 27002.*

Tabla 6: Medidas descriptivas de usuarios que piden su contraseña con opción a cambio.

6. PIDEN SU CONTRASEÑA CON OPCION A CAMBIO

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	20	50,0	50,0	50,0
	ALGUNAS VECES	10	25,0	25,0	75,0
	SIEMPRE	10	25,0	25,0	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 6: Porcentaje de usuarios que piden su contraseña con opción a cambio.

Se verifican usuarios que siempre solicitan su reseteo de contraseña con opción a cambio y otro alto porcentaje que lo hace algunas veces y nunca, lo que hace vulnerable la seguridad de información del equipo ya que por defecto muchas veces las contraseñas que brinda el CDS son las mismas para todos los usuarios y si el usuario no la cambia por parte propia cualquier usuario puede ingresar a sus equipos teniendo libertad de ingresar. El pedido de cambio de contraseña con opción a cambio es responsabilidad del usuario ya que CDS siempre consulta el tipo de reseteo que desea (Con y sin opción a cambio).

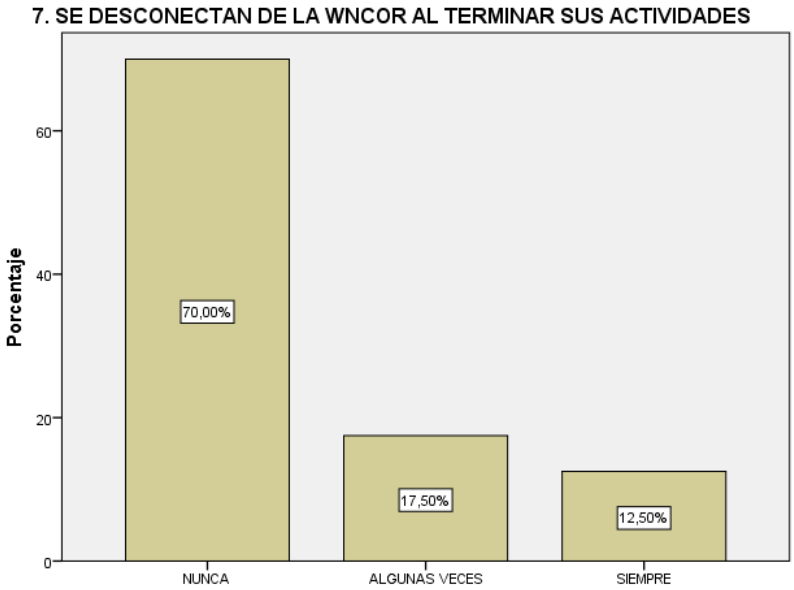
PREGUNTA 7: ***¿Te desconectas de la Wncor cuando acabas tus actividades?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que se desconectan de la Wncor al terminar sus actividades antes de aplicarse la *NTP ISO/IEC 27002.*

Tabla 7: Medidas descriptivas de usuarios que se desconectan de la Wncor al terminar sus actividades.

7. SE DESCONECTAN DE LA WNCOR AL TERMINAR SUS ACTIVIDADES

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	28	70,0	70,0	70,0
	ALGUNAS VECES	7	17,5	17,5	87,5
	SIEMPRE	5	12,5	12,5	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 7: Porcentaje de usuarios que se desconectan de la Wncor al terminar sus actividades.

Se presenta un alto porcentaje de usuarios que no se desconectan de la Wncor para conectarse al cable de red, sólo el 12,50% lo hace y la diferencia está entre Algunas veces y Nunca, lo que provoca se tenga un alto reporte de incidencias por problemas a los ingresos a la Wncor y a file Servers ya que el sistema confunde el tipo de red que se estará utilizando y no logra conectarse de forma correcta, alterando el tráfico de datos y afectando la conectividad a los aplicativos.

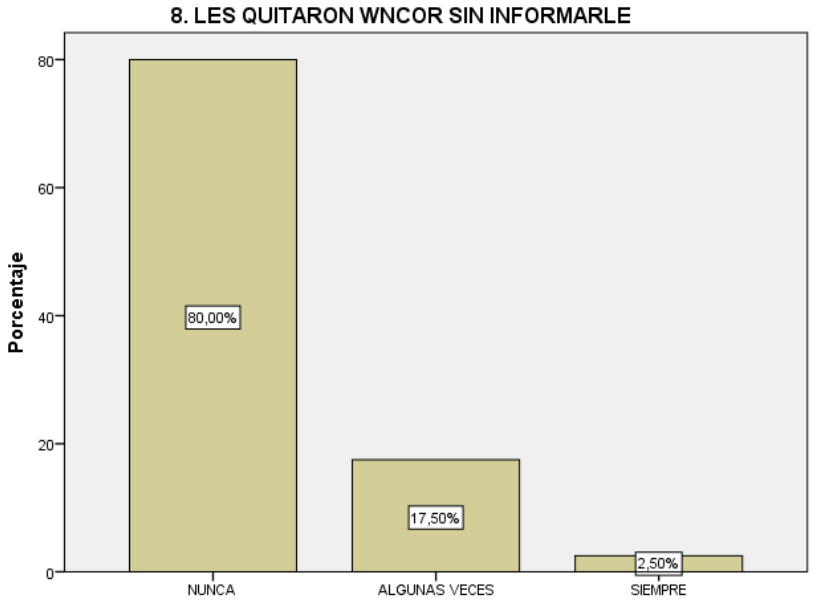
PREGUNTA 8: ***¿Te quitaron el acceso a Wncor sin informarte?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que les quitaron Wncor sin informarles antes de aplicarse la *NTP ISO/IEC 27002.*

Tabla 8: Medidas descriptivas de usuarios que les quitaron Wncor sin informarles.

8. LES QUITARON WNCOR SIN INFORMARLE

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	32	80,0	80,0	80,0
	ALGUNAS VECES	7	17,5	17,5	97,5
	SIEMPRE	1	2,5	2,5	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 8: Porcentaje de usuarios que les quitaron Wncor sin informarles.

En el presente gráfico no se muestra alto peligro de incidencia con conexión a la Wncor y a File server ya que los usuarios no fueron altamente afectados por que no se les quitó el acceso a la Wncor sin informar, es poco probable que pasen estos casos, pero si han ocurrido y en ellos muchos usuarios han intentado muchas veces conectarse sin éxito porque nunca se le informa al usuario si se les quitó algún acceso más sólo cuando se les brinda. El resultado final para un usuario que no cuenta con acceso sin saberlo será los constantes intentos fallidos que reportará al CDS y recientemente el CDS le informará que ya no cuenta con accesos.

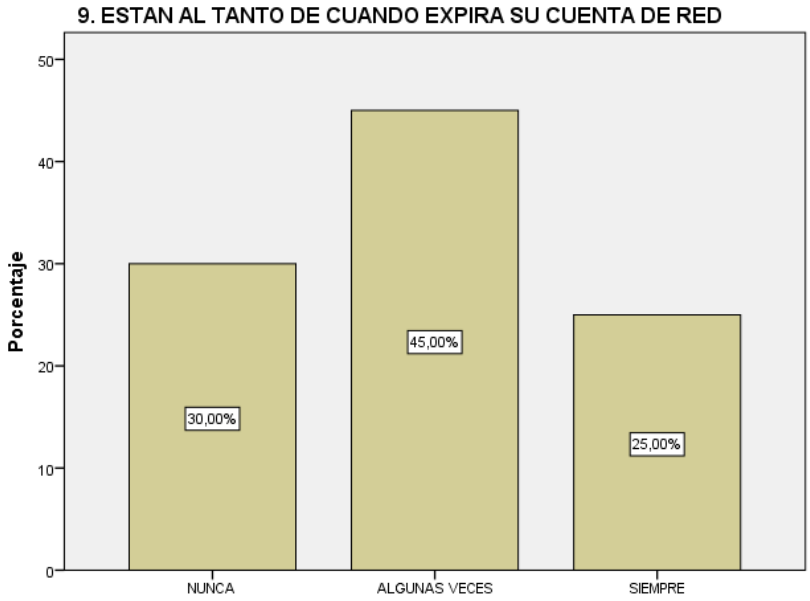
PREGUNTA 9: ***¿Estas al tanto de cuando expira tu cuenta de red?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que están al tanto de cuando expira su cuenta de red antes de aplicarse la *NTP ISO/IEC 27002.*

Tabla 9: Medidas descriptivas de usuarios que están al tanto de cuando expira su cuenta de red.

9. ESTAN AL TANTO DE CUANDO EXPIRA SU CUENTA DE RED

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	12	30,0	30,0	30,0
	ALGUNAS VECES	18	45,0	45,0	75,0
	SIEMPRE	10	25,0	25,0	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 9: Porcentaje de usuarios que están al tanto de cuando expira su cuenta de red.

Se puede demostrar la cantidad de usuarios que no toman en cuenta la fecha en que expira su cuenta de red que es muy distinto a que expire su clave de red, ya que al expirar la cuenta quiere decir que la cuenta ya se encuentra desactivada, y con ello se desactivan todos los accesos del usuario entre ellos el acceso a la Wncor y al file server y es esa una de las causas que presentan las incidencias, los usuarios son informados el día de la creación de su cuenta la fecha de expiración, sin embargo se verifica en el gráfico el desinterés que tiene.

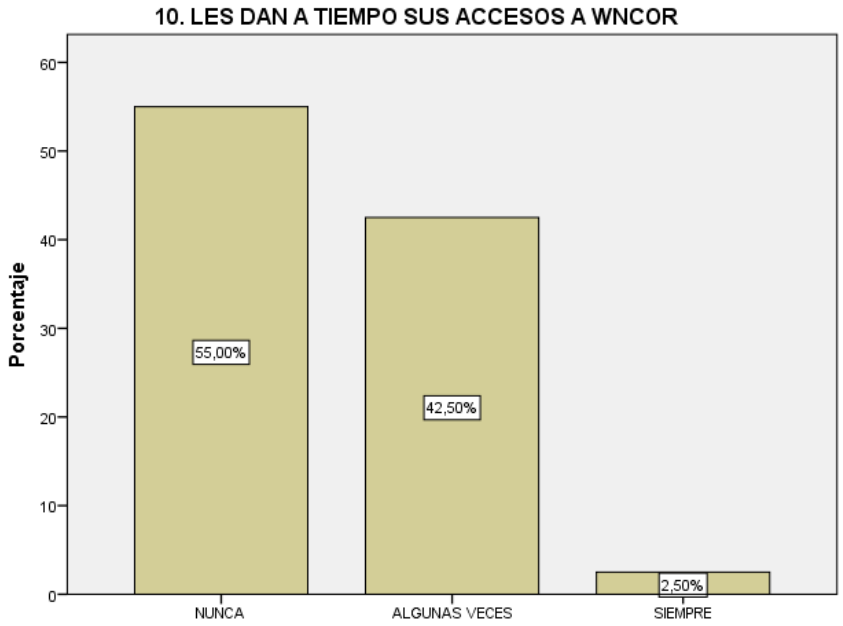
PREGUNTA 10: ***¿Cuándo pides tus accesos a Wncor te lo dan a tiempo?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que les dan a tiempo sus accesos a Wncor antes de aplicarse la *NTP ISO/IEC 27002.*

Tabla 10: Medidas descriptivas de usuarios que les dan a tiempo sus accesos a Wncor.

10. LES DAN A TIEMPO SUS ACCESOS A WNCOR

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	22	55,0	55,0	55,0
	ALGUNAS VECES	17	42,5	42,5	97,5
	SIEMPRE	1	2,5	2,5	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 10: Porcentaje de usuarios que les dan a tiempo sus accesos a Wncor.

Se demuestra en el gráfico una gran cantidad de usuarios que indicaron que no se les brindaron sus accesos a Wncor en el tiempo correcto, uno de los defectos de los usuarios de Interbank es que solicitan sus accesos a última hora, es por ello que muchos usuarios sólo solicitan, tomando este caso el acceso a Wncor pero no tienen la confirmación de ya tenerlos, sin embargo reportan al CDS que no pueden ingresar, una mala práctica de realizar intentos fallidos sin tener la confirmación de los accesos pero de insistir.

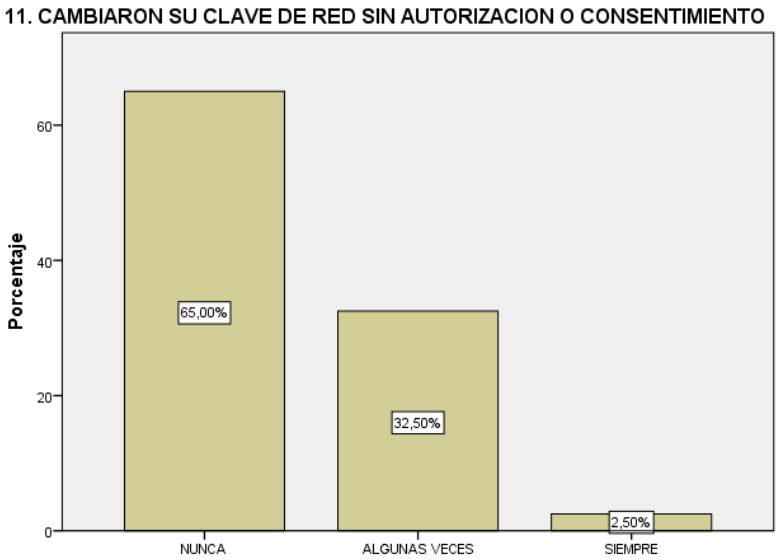
PREGUNTA 11: ***¿Cambiaron tu clave de red sin tu autorización o consentimiento?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que les cambiaron su clave de red sin autorización o consentimiento antes de aplicarse la *NTP ISO/IEC 27002.*

Tabla 11: Medidas descriptivas de usuarios que les cambiaron su clave de red sin autorización o consentimiento.

11. CAMBIARON SU CLAVE DE RED SIN AUTORIZACION O CONSENTIMIENTO

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	26	65,0	65,0	65,0
	ALGUNAS VECES	13	32,5	32,5	97,5
	SIEMPRE	1	2,5	2,5	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 11: Porcentaje de usuarios que les cambiaron su clave de red sin autorización o consentimiento.

Teniendo en cuenta los gráficos anteriores, se muestran usuarios a quienes si les cambiaron su clave de red sin su autorización o consentimiento, provocando en un primer intento no lograr iniciar sesión y corriendo el riesgo de tener perdida o fuga de información, lo que conlleva también a que los usuarios tengan que cambiar su contraseña y no puedan ingresar al file server o conectarse a Wncor en un primer intento pues tiene que reiniciar la PC para que la clave principal sea aceptada.

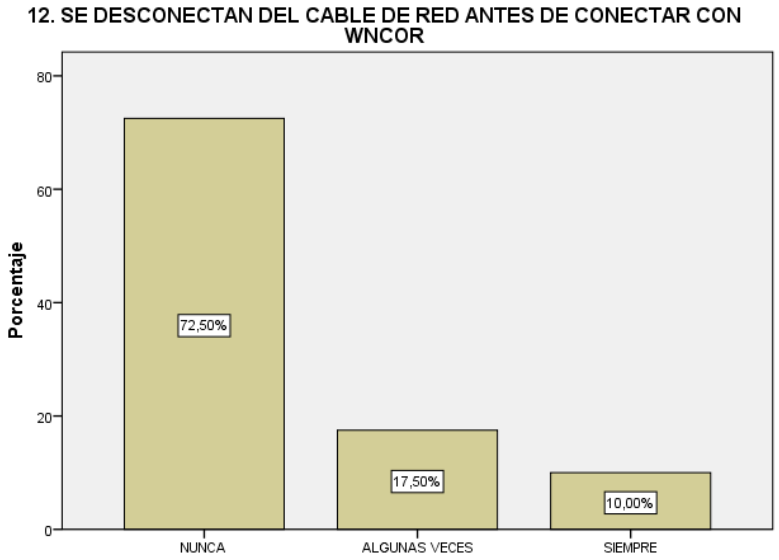
PREGUNTA 12: ***¿Antes de conectar a Wncor te desconectas del cable red?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que se desconectan del cable de red antes de conectar con Wncor antes de aplicarse la *NTP ISO/IEC 27002.*

Tabla 12 : Medidas descriptivas de usuarios que se desconectan del cable de red antes de conectar con Wncor.

12. SE DESCONECTAN DEL CABLE DE RED ANTES DE CONECTAR CON WNCOR

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	29	72,5	72,5	72,5
	ALGUNAS VECES	7	17,5	17,5	90,0
	SIEMPRE	4	10,0	10,0	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 12: Porcentaje de usuarios que se desconectan del cable de red antes de conectar con Wncor.

El gráfico presenta una gran cantidad de usuario que por facilidad de su trabajo prefieren no desconectarse de la Wncor, pero muchos de ellos llevan sus laptop fuera y se conectan a otras redes inalámbricas, logrando des configurar la conexión que su laptop ya tiene para la red Wncor, lo que provoca al momento de volver a querer conectarse que se sufra incidencia y no logre conectarse, o pueda conectarse solo en modo red, sufriendo retrasos en sus actividades ya que se tiene que realizar la reconfiguración de la Wncor para la correcta conexión.

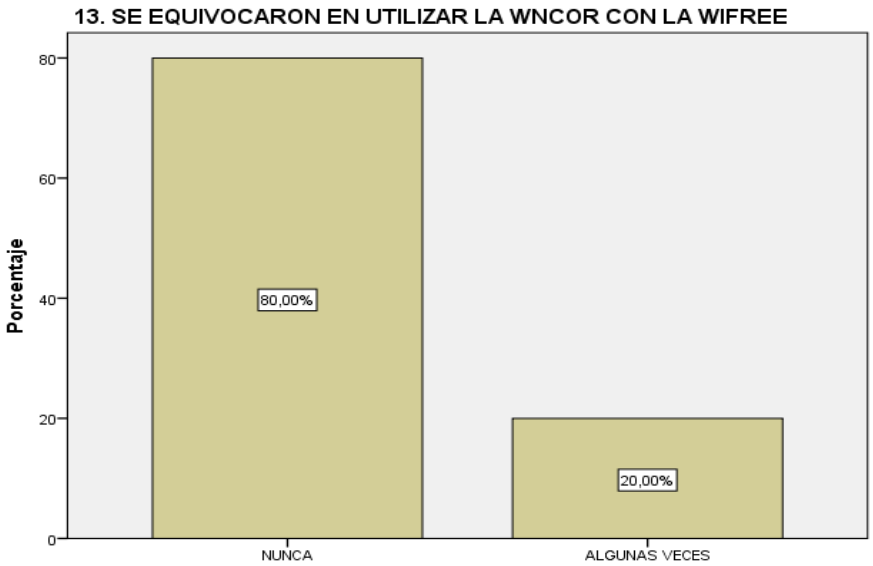
PREGUNTA 13: ***¿Te has equivocado en utilizar la Wncor con la Wifree?***

Los resultados de la prueba indican en el siguiente cuadro el porcentaje de usuarios que se equivocaron en utilizar la Wncor con la Wifree antes de aplicarse la *NTP ISO/IEC 27002*.

Tabla 13: Medidas descriptivas de usuarios que se equivocaron en utilizar la Wncor con la wifree.

13. SE EQUIVOCARON EN UTILIZAR LA WNCOR CON LA WIFREE

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	32	80,0	80,0	80,0
	ALGUNAS VECES	8	20,0	20,0	100,0
	Total	40	100,0	100,0	



Fuente: Elaboración Propia

Figura 13: Porcentaje de usuarios que se equivocaron en utilizar la Wncor con la wifree.

La red Wncor y la Red Wifree son redes completamente distintas, pero ambas son parte de Interbank lo que ocasiona que muchos usuarios se confundan al conectarse. Aunque el resultado no es mucho se muestran usuario que, si han cometido el error de conectarse a la Wifree y desde ahí querer ingresar a los File Server causándoles incidencias por no poder ingresar, una mala práctica de los usuarios pues se les instruye siempre antes de conectarse por primera vez a la Wncor, pero el Wifree tiene el libre acceso a Internet es esa una de las causas que lo eligen.

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS.

De acuerdo a los indicadores **fallas de conexión a red Wncor** y **fallas de ingreso a file server** se implementaron las preguntas para la encuesta, de las cuales verificamos que cada una podía tener correlación con la otra y que correlacionándolas podíamos resolver hasta dos o más problemas aplicando las buenas practicas que la norma ISO 27002 nos brinda, es por ello que seleccionamos para cada pregunta una dimensión, propuestas por las propiedades de un sistema de información seguro. Una vez descubierta la correlación que tienen nuestras dimensiones elegiremos las normas correctas para la implementación de nuestro modelo.

PREGUNTAS	DIMENSIONES
1. *¿Alguna vez has brindado tu clave de red a otro usuario?*	***CONFIDENCIALIDAD***
2. *¿Bloqueas tu pc cuando sales de tu sitio?*	***RESPONSABILIDAD***
3. *¿Prestaste tu equipo a otro usuario?*	***RESPONSABILIDAD***
4. *¿Cierras la sesión de tu equipo al final del día?*	***RESPONSABILIDAD***
5. *¿Le das importancia a las notificaciones de cambio de contraseña?*	***CONFIDENCIALIDAD***
6. *¿Pides tú contraseña con opción a cambio al Centro De Servicios?*	***CONFIDENCIALIDAD***
7. *¿Te desconectas de la Wncor cuando acabas tus actividades?*	***COMPROMISO***
8. *¿Te quitaron el acceso a Wncor sin informarte?*	***ACCESIBILIDAD***
9. *¿Estas al tanto de cuando expira tu cuenta de red?*	***CONFIDENCIALIDAD***
10. *¿Cuándo pides tus accesos te lo dan a tiempo?*	***ACCESIBILIDAD***
11. *¿Cambiaron tu clave de red sin tu autorización o consentimiento?*	***CONFIDENCIALIDAD***
12. *¿Antes de conectar a Wncor te desconectas del cable red?*	***COMPROMISO***
13. *¿Te has equivocado en utilizar la Wncor con la Wifree?*	***COMPROMISO***

Se sospecha que cada dimensión tiene correlación con otra, por ello se muestra a continuación el proceso de investigación para saber qué tan relacionada está una dimensión con otra aplicando las técnicas indicadas en el procesamiento de datos.

Una vez obtenidas el porcentaje de relación que estas dimensiones tienen podremos elegir las normas correctas para la implementación de nuestro modelo.

a) Correlación de dimensiones para la implementación del modelo:

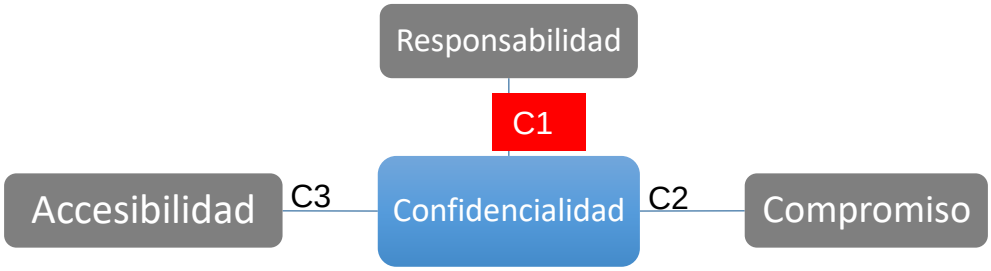


Figura 14: Teoría de variables

Resultados en tablas y figuras

Correlación	Relación	Formulación
C1	Confidencialidad →Responsabilidad	La Responsabilidad tiene una influencia positiva sobre la Confidencialidad.

Tabla 14: Calculo del coeficiente de Alfa de Cronbach

Cálculo del coeficiente de *Alfa de Cronbach* para medir la fiabilidad de las preguntas y correlación de los ítems donde nos dará una solidez interna y donde se medirán las variables de *Confidencialidad* y *Responsabilidad*.

Resumen de procesamiento de casos

		N	%
Casos	Válido	40	100,0
	Excluido[a]	0	,0
	Total	40	100,0

(**Fuente**: elaboración propia)

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,563	,593	2

(**Fuente**: elaboración propia)

En el resultado observamos un valor de **59.3%**≈60% lo cual podemos empezar a decir que internamente existe una sólida relación entre los compuestos o variables a estudiar.

Tabla 15: Tabla recuento de contingencia aplicada a las preguntas de las dimensiones Confidencialidad y Responsabilidad.

Tabla cruzada BRINDARON SU CLAVE DE RED A OTRO USUARIO*PRESTAN SU EQUIPO A OTROS USUARIO

Recuento

		PRESTAN SU EQUIPO A OTROS USUARIO		
		NUNCA	ALGUNAS VECES	Total
BRINDARON SU CLAVE DE RED A OTRO USUARIO	NUNCA	13	8	21
	ALGUNAS VECES	4	14	18
	SIEMPRE	0	1	1
Total		17	23	40

(**Fuente**: elaboración propia)

Tabla 16: Tabla de contingencia aplicada a las preguntas de las dimensiones Confidencialidad y Responsabilidad.

Tabla cruzada PRESTAN SU EQUIPO A OTROS USUARIO*BRINDARON SU CLAVE DE RED A OTRO USUARIO

		BRINDARON SU CLAVE DE RED A OTRO USUARIO			
		NUNCA	ALGUNAS VECES	SIEMPRE	Total
PRESTAN SU EQUIPO A OTROS USUARIO	NUNCA	13	4	0	17
		76,5%	23,5%	0,0%	100,0%
	ALGUNAS VECES	8	14	1	23
		34,8%	**60,9%**	4,3%	100,0%
Total		21	18	1	40
		52,5%	45,0%	2,5%	100,0%

(**Fuente**: elaboración propia)

Del total de encuestados, el 76% de personas que están de acuerdo con que Nunca brindaron su clave de Red a otro Usuarios y están de acuerdo con que Nunca prestan su Equipo a otros usuarios, por lo que tenemos una sospecha de que estas variables estén relacionadas positivamente y podríamos identificar hasta qué grado estarían relacionadas.

Tabla 17: Tabla de Contingencia sobre las variables Confidencialidad y Responsabilidad.

Previamente se realizó el cálculo de las variables según las dimensiones estudiadas en el instrumento.

Tabla cruzada Grado de Confidencialidad (Agrupada)*Grado de Responsabilidad (Agrupada)

			Grado de Responsabilidad (Agrupada)			
			Nunca	Algunas veces	Siempre	Total
Grado de Confidencialidad (Agrupada)	Nunca		12	7	0	19
			63,2%	36,8%	0,0%	100,0%
	Algunas veces		3	5	2	10
			30,0%	**50,0%**	20,0%	100,0%
	Siempre		1	10	0	11
			9,1%	**90,9%**	0,0%	100,0%
Total			16	22	2	40
			40,0%	55,0%	5,0%	100,0%

(**Fuente**: elaboración propia)

Observamos según la tabla de doble entrada que las variables muestran un indicio de relación positiva en cuanto aquellos que afirman que nunca brindan su clave de Red también están de acuerdo con que no prestan su equipo siendo estos un 63.2%.

Tabla 18: Pruebas de Chi Cuadrado.

Empezaremos demostrando que las Variables *Confidencialidad* y *Responsabilidad* no son independientes y están correlacionadas, para dicha demostración usaremos la prueba estadística no paramétrica **Chi-Cuadrado** donde lo que nos va ayudar es a definir si tienen relación.

Por lo que según la prueba se inicia planteando dos Hipótesis:

H_0: *La variable Responsabilidad es independiente de la variable confidencialidad*

H_1: *La variable Responsabilidad depende de la variable confidencialidad*

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	7,004[a]	2	**,030**
Razón de verosimilitud	7,569	2	,023
Asociación lineal por lineal	6,733	1	,009
N de casos válidos	40		

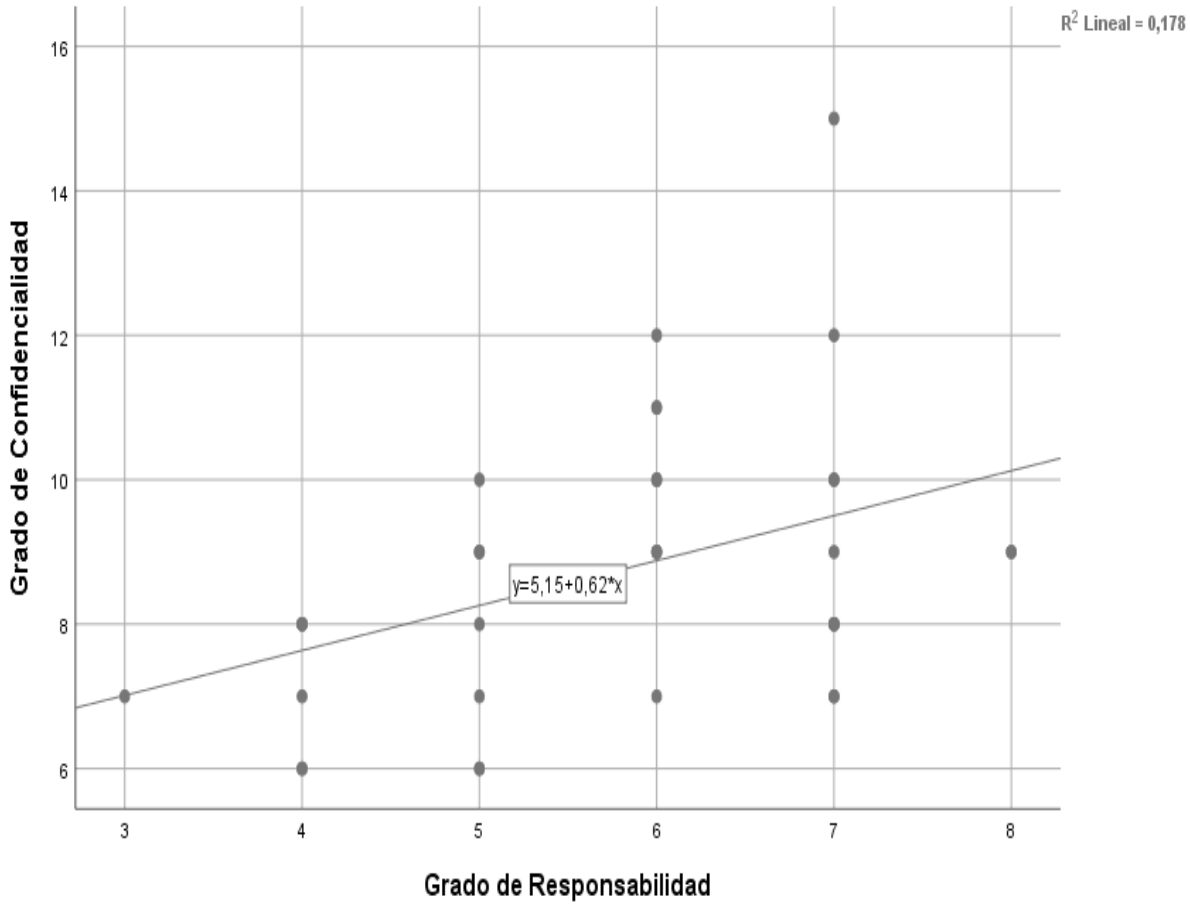
a. 2 casillas (33.3%) han esperado un recuento menor que 5. El recuento mínimo esperado es .43.

(**Fuente**: elaboración propia)

De acuerdo al resultado de la prueba nos arroja un valor de **0.039 << 0.5** mucho menor al 5% por lo cual se rechaza la Hipótesis nula de la prueba y concluimos y se demuestra que las variables están relacionas.

Figura 15: Grado de confidencialidad y responsabilidad

Gráfico de regresión Lineal simple para dos variables cuantitativas donde nos ayudara a demostrar si la relación que se mantiene en las variables es positiva (Se transformaron las variables cualitativas a cuantitativas.)



(**Fuente**: elaboración propia)

Según el gráfico de dispersión lineal observamos que las variables *Confidencialidad* y *Responsabilidad* están relacionadas positivamente con un grado de relación de R2=20% (Índice bajo debido a la cantidad de muestra encuestada por lo que usaremos pruebas más robustas para medir el grado de relación que estas mantienen.)

Tabla 19: Tabla de correlación No paramétrica usando la prueba de Rho de Spearman entre las variables Confidencialidad y Responsabilidad

Correlaciones no paramétricas

Correlaciones

			Grado de Confidencialidad	Grado de Responsabilidad
Rho de Spearman	Grado de Confidencialidad	Coeficiente de correlación	1,000	,413**
		Sig. (bilateral)	.	,008
		N	40	40
	Grado de Responsabilidad	Coeficiente de correlación	,413**	1,000
		Sig. (bilateral)	,008	.
		N	40	40

**. La correlación es significativa en el nivel 0,01 (bilateral).

(**Fuente**: elaboración propia)

Tabla 20: Tabla de correlación No paramétrica usando la prueba de prueba de correlación de Pearson entre las variables Confidencialidad y Responsabilidad

Correlaciones

		Grado de Confidencialidad	Grado de Responsabilidad
Grado de Confidencialidad	Correlación de Pearson	1	,421**
	Sig. (bilateral)		,007
	N	40	40
Grado de Responsabilidad	Correlación de Pearson	,421**	1
	Sig. (bilateral)	,007	
	N	40	40

**. La correlación es significativa en el nivel 0,01 (bilateral).

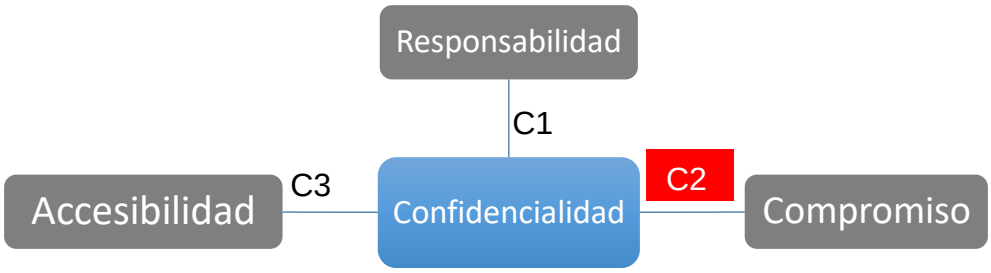
(**Fuente**: elaboración propia)

Según los resultados del programa para la prueba de correlación nos arrojan un 41.3% y 42.1% para Rho de Spearman y Pearson respectivamente. Siendo un grado de relación significante entre las variables por lo que podemos ir concluyendo que ambas variables están relacionadas positivamente a un 42.1%.

Deducción de correlación para C1: *La Responsabilidad tiene una influencia positiva sobre la Confidencialidad.*

Según los resultados se demuestra según la prueba chi-cuadrado que las variables Responsabilidad y Confidencialidad están relacionadas y con la prueba de Pearson demostramos que están correlacionas un **42.1%** positivamente por lo que según nuestro objetivo de Implementar un modelo de buenas prácticas aplicando la Norma ISO 27002 para mejorar la gestión de incidencias de la red Wncor nos enfocaremos según nuestro modelo a buscar normas y controles la cual nos ayuden a aumentar el valor de responsabilidad de los usuarios para buscar atacar de manera indirecta el grado de confidencialidad que estas deberían tener y así generar menor número de incidencias por el problema latente.

b) Correlación de dimensiones para la implementación del modelo:



Resultados en tablas y figuras

Correlación	Relación	Formulación
C2	Confidencialidad →Compromiso	El Compromiso tiene una influencia positiva sobre la Confidencialidad.

Tabla 21: Calculo del coeficiente de Alfa de Cronbach

Para medir la fiabilidad de las preguntas y correlación de los ítems donde nos dará una solidez interna y donde se medirán las variables de *Confidencialidad* y *Compromiso*.

Resumen de procesamiento de casos

		N	%
Casos	Válido	40	100,0
	Excluido[a]	0	,0
	Total	40	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

(**Fuente**: elaboración propia)

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,562	,634	2

(**Fuente**: elaboración propia)

En el resultado observamos un valor de **63.4%**≈63% lo cual podemos empezar a decir que internamente existe una sólida relación entre los compuestos o variables a estudiar.

Tabla 22: Tabla recuento de contingencia aplicada a las preguntas de las dimensiones Confidencialidad y Compromiso.

Tabla cruzada SE DESCONECTAN DEL CABLE DE RED ANTES DE CONECTAR A LA WNCOR*BRINDARON SU CLAVE DE RED A OTRO USUARIO

Recuento

		BRINDARON SU CLAVE DE RED A OTRO USUARIO			
		NUNCA	ALGUNAS VECES	SIEMPRE	Total
SE DESCONECTAN DEL CABLE DE RED ANTES DE CONECTAR A LA WNCOR	NUNCA	18	11	0	29
	ALGUNAS VECES	3	4	0	7
	SIEMPRE	0	3	1	4
Total		21	18	1	40

(**Fuente**: elaboración propia)

Tabla 23: Tabla de contingencia aplicada a las preguntas de las dimensiones Confidencialidad y Compromiso.

Tabla cruzada BRINDARON SU CLAVE DE RED A OTRO USUARIO*SE DESCONECTAN DEL CABLE DE RED ANTES DE CONECTAR A LA WNCOR

			SE DESCONECTAN DEL CABLE DE RED ANTES DE CONECTAR A LA WNCOR			
			NUNCA	ALGUNAS VECES	SIEMPRE	Total
BRINDARON SU CLAVE DE RED A OTRO USUARIO	NUNCA		18	3	0	21
			85,7%	14,3%	0,0%	100,0%
	ALGUNAS VECES		11	4	3	18
			61,1%	**22,2%**	16,7%	100,0%
	SIEMPRE		0	0	1	1
			0,0%	0,0%	**100,0%**	100,0%
Total			29	7	4	40
			72,5%	17,5%	10,0%	100,0%

(**Fuente**: elaboración propia)

Del total de encuestados, el **85.7%** de personas que están de acuerdo con que Nunca brindaron su clave de Red a otro Usuarios están de acuerdo con que Nunca se desconectan del cable de red al conectarse a la Wncor, por lo que tenemos una sospecha de que estas variables estén relacionadas positivamente y podríamos identificar hasta qué grado estarían relacionadas.

Tabla 24: Tabla de Contingencia sobre las variables Confidencialidad y Compromiso.

Previamente se realizó el cálculo de las variables según las dimensiones estudiadas en el instrumento.

Tabla cruzada Grado de Confidencialidad (Agrupada)*Grado de Compromiso (Agrupada)

			Grado de Compromiso (Agrupada)			
			Nunca	Algunas veces	Siempre	Total
Grado de Confidencialidad (Agrupada)	Nunca		14	5	0	19
			73,7%	26,3%	0,0%	100,0%
	Algunas veces		9	1	0	10
			90,0%	**10,0%**	0,0%	100,0%
	Siempre		5	2	4	11
			45,5%	18,2%	**36,4%**	100,0%
Total			28	8	4	40
			70,0%	20,0%	10,0%	100,0%

(**Fuente**: elaboración propia)

Observamos según la tabla de doble entrada que las variables muestran un indicio de relación positiva, como por ejemplo aquellos que afirman que nunca brindan su clave de Red también están de acuerdo con que no se desconectan del cable de red al conectarse a la wncor siendo estos un 73.7%.

Tabla 25: Variables Confidencialidad y Compromiso no son independientes y están correlacionadas.

Empezaremos demostrando que las Variables *Confidencialidad* y *Compromiso* no son independientes y están correlacionadas, para dicha demostración usaremos la prueba estadística no paramétrica **Chi-Cuadrado** donde lo que nos va ayudar es a definir si tienen relación.

Por lo que según la prueba se inicia planteando dos Hipótesis:

H_0: *La variable Compromiso es independiente de la variable confidencialidad*

H_1: *La variable Compromiso depende de la variable confidencialidad*

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	12,998[a]	4	**,011**
Razón de verosimilitud	12,947	4	,012
Asociación lineal por lineal	5,246	1	,022
N de casos válidos	40		

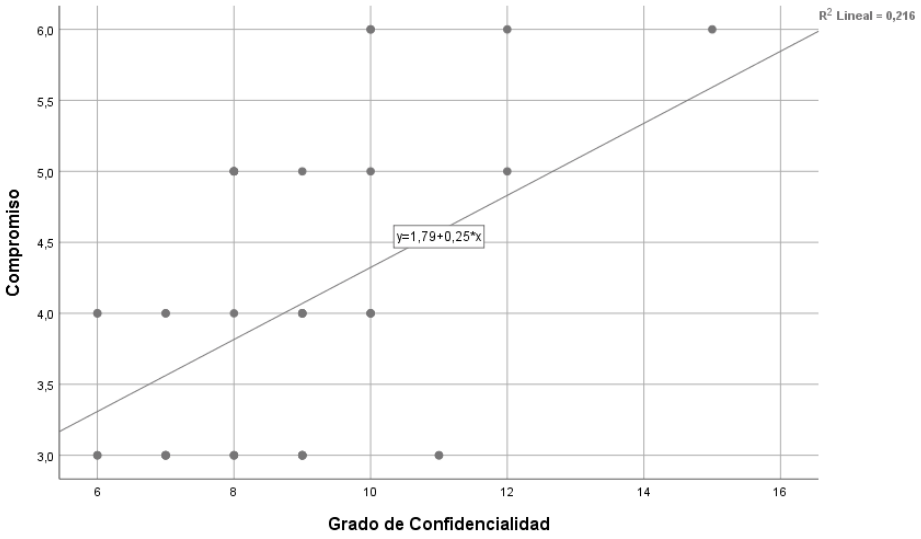
a. 6 casillas (66,7%) han esperado un recuento menor que 5. El recuento mínimo esperado es 1,00.

(**Fuente**: elaboración propia)

De acuerdo al resultado de la prueba nos arroja un valor de **0.11 << 0.5** mucho menor al 5% por lo cual se rechaza la Hipótesis nula de la prueba y concluimos y se demuestra que las variables están relacionas.

Figura 16: Gráfico de regresión Lineal simple para dos variables cuantitativas.

Donde nos ayudara a demostrar si la relación que se mantiene en las variables es positiva (Se transformaron las variables cualitativas a cuantitativas.)



(**Fuente**: elaboración propia)

Según el gráfico de dispersión lineal observamos que las variables *Confidencialidad* y *Compromiso* están relacionadas positivamente con un grado de relación de R2=21% (Índice bajo debido a la cantidad de muestra encuestada por lo que usaremos pruebas más robustas para medir el grado de relación que estas mantienen.)

Tabla 26: Tabla de correlación No paramétrica usando la prueba de Rho de Spearman entre las variables Confidencialidad y Responsabilidad.

Correlaciones no paramétricas

Correlaciones

			Grado de Confidencialidad	Grado de Compromiso
Rho de Spearman	Grado de Confidencialidad	Coeficiente de correlación	1,000	,359*
		Sig. (bilateral)	.	,023
		N	40	40
	Grado de Compromiso	Coeficiente de correlación	,359*	1,000
		Sig. (bilateral)	,023	.
		N	40	40

*. La correlación es significativa en el nivel 0,05 (bilateral).

(**Fuente**: elaboración propia)

Tabla 27: Tabla de correlación No paramétrica usando la prueba de prueba de correlación de Pearson entre las variables Confidencialidad y Responsabilidad.

Correlaciones

		Grado de Confidencialidad	Grado de Compromiso
Grado de Confidencialidad	Correlación de Pearson	1	,464**
	Sig. (bilateral)		,003
	N	40	40
Grado de Compromiso	Correlación de Pearson	,464**	1
	Sig. (bilateral)	,003	
	N	40	40

**. La correlación es significativa en el nivel 0,01 (bilateral).

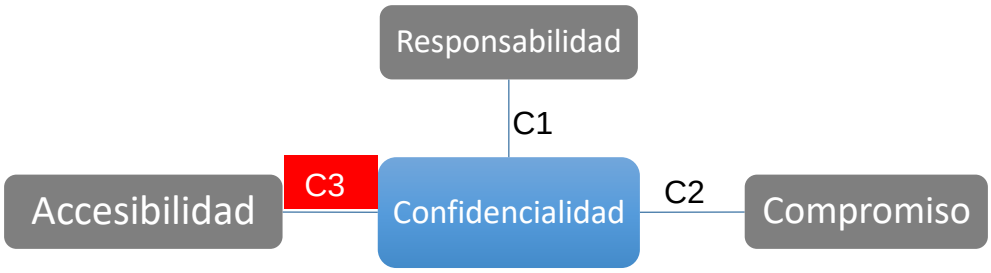
(**Fuente**: elaboración propia)

Según los resultados del programa para las pruebas de correlación nos arrojan un 35.9% y 46.4% para Rho de Spearman y Pearson respectivamente. Siendo un grado de relación significante entre las variables por lo que podemos ir concluyendo que ambas variables están relacionadas positivamente a un 46.4%.

Deducción de correlación para C2: *El Compromiso tiene una influencia positiva sobre la Confidencialidad.*

Según los resultados se demuestra según la prueba chi-cuadrado que las variables Compromiso y Confidencialidad están relacionadas y con la prueba de Pearson demostramos que están correlacionas un **46.4%** positivamente por lo que según nuestro objetivo de Implementar un modelo de buenas prácticas aplicando la Norma ISO 27002 para mejorar la gestión de incidencias de la red Wncor nos enfocaremos según nuestro modelo a buscar normas la cual nos ayuden a aumentar el valor de Compromiso de los usuarios para buscar atacar de manera indirecta el grado de confidencialidad que estas deberían tener y así generar menor número de incidencias por el problema latente.

c) Correlación de dimensiones para la implementación del modelo:



Resultados en tablas y figuras

Teoría	Relación	Formulación
C3	Confidencialidad →Accesibilidad	La Accesibilidad tiene una influencia positiva sobre la Confidencialidad.

Tabla 28: Calculo del coeficiente de Alfa de Cronbach.

Para medir la fiabilidad de las preguntas y correlación de los ítems donde nos dará una solidez interna y donde se medirán las variables de *Confidencialidad* y *Accesibilidad*.

Resumen de procesamiento de casos

		N	%
Casos	Válido	40	100,0
	Excluido[a]	0	,0
	Total	40	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

(**Fuente**: elaboración propia)

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,556	,725	2

(**Fuente**: elaboración propia)}

En el resultado observamos un valor de **72.5%**≈73% lo cual podemos empezar a decir que internamente existe una sólida relación entre los compuestos o variables a estudiar.

Tabla 29: Tabla recuento de contingencia aplicada a las preguntas de las dimensiones Confidencialidad y Accesibilidad

Tabla cruzada BRINDARON SU CLAVE DE RED A OTRO USUARIO*LE QUITARON WNCOR SIN INFORMARLE

Recuento

		LE QUITARON WNCOR SIN INFORMARLE			
		NUNCA	ALGUNAS VECES	SIEMPRE	Total
BRINDARON SU CLAVE DE RED A OTRO USUARIO	NUNCA	21	0	0	21
	ALGUNAS VECES	11	7	0	18
	SIEMPRE	0	0	1	1
Total		32	7	1	40

(**Fuente**: elaboración propia)

Tabla 30: Tabla de contingencia aplicada a las preguntas de las dimensiones Confidencialidad y Accesibilidad.

Tabla cruzada BRINDARON SU CLAVE DE RED A OTRO USUARIO*LE QUITARON WNCOR SIN INFORMARLE

			LE QUITARON WNCOR SIN INFORMARLE			
			NUNCA	ALGUNAS VECES	SIEMPRE	Total
BRINDARON SU CLAVE DE RED A OTRO USUARIO	NUNCA		21	0	0	21
			100,0%	0,0%	0,0%	100,0%
	ALGUNAS VECES		11	7	0	18
			61,1%	**38,9%**	0,0%	100,0%
	SIEMPRE		0	0	1	1
			0,0%	0,0%	100,0%	100,0%
Total			32	7	1	40
			80,0%	17,5%	2,5%	100,0%

(**Fuente**: elaboración propia)

Del total de encuestados, el 61.1% de personas que están de acuerdo con que Algunas veces brindaron su clave de Red a otro Usuarios están de acuerdo con que Nunca les han quitado la Wncor sin informarle, por lo que tenemos una sospecha de que estas variables estén relacionadas positivamente y podríamos identificar hasta qué grado estarían relacionadas.

Tabla 31: Tabla de Contingencia sobre las variables Confidencialidad y Accesibilidad.

Previamente se realizó el cálculo de las variables según las dimensiones estudiadas en el instrumento.

Tabla cruzada Grado de Confidencialidad (Agrupada)*Grado de Accesibilidad (Agrupada)

			Grado de Accesibilidad (Agrupada)			
			Nunca	Algunas veces	Siempre	Total
Grado de Confidencialidad (Agrupada)	Nunca	11	8	0	19
		57,9%	42,1%	0,0%	100,0%
	Algunas veces	3	7	0	10
		30,0%	**70,0%**	0,0%	100,0%
	Siempre	3	4	4	11
		27,3%	36,4%	**36,4%**	100,0%
Total		17	19	4	40
		42,5%	47,5%	10,0%	100,0%

(**Fuente**: elaboración propia)

Observamos según la tabla de doble entrada que las variables muestran un indicio de relación positiva en cuanto aquellos que afirman que nunca brindan su clave de Red también están de acuerdo con que no les han quitado sus accesos a la Wncor sin avisarles siendo estos un 57.9%.

Tabla 32: Variables Confidencialidad y Accesibilidad no son independientes y están correlacionadas.

Empezaremos demostrando que las Variables *Confidencialidad* y *Accesibilidad* no son independientes y están correlacionadas, para dicha demostración usaremos la prueba estadística no paramétrica **Chi-Cuadrado** donde lo que nos va ayudar es a definir si tienen relación.

Por lo que según la prueba se inicia planteando dos Hipótesis:

H_0: *La variable Accesibilidad es independiente de la variable confidencialidad*

H_1: *La variable Accesibilidad depende de la variable confidencialidad*

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	14,042[a]	4	**,007**
Razón de verosimilitud	13,740	4	,008
Asociación lineal por lineal	7,233	1	,007
N de casos válidos	40		

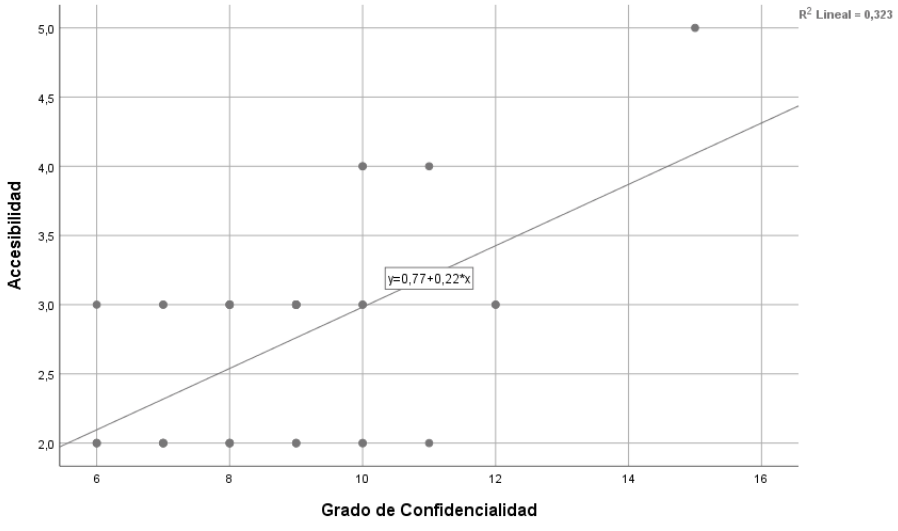
a. 6 casillas (66,7%) han esperado un recuento menor que 5. El recuento mínimo esperado es 1,00.

(**Fuente**: elaboración propia)

De acuerdo al resultado de la prueba nos arroja un valor de **0.007 << 0.5** mucho menor al 5% por lo cual se rechaza la Hipótesis nula de la prueba y concluimos y se demuestra que las variables están relacionas.

Imagen 17: Gráfico de regresión Lineal simple

Para dos variables cuantitativas donde nos ayudará a demostrar si la relación que se mantiene en las variables es positiva (Se transformaron las variables cualitativas a cuantitativas.)



(**Fuente**: elaboración propia)

Según el gráfico de dispersión lineal observamos que las variables *Confidencialidad* y *Accesibilidad* están relacionadas positivamente con un grado de relación de R2=32% (Índice bajo debido a la cantidad de muestra encuestada por lo que usaremos pruebas más robustas para medir el grado de relación que estas mantienen.)

Tabla 33: Tabla de correlación No paramétrica usando la prueba de Rho de Spearman entre las variables Confidencialidad y Accesibilidad

Correlaciones no paramétricas

Correlaciones

			Grado de Confidencialidad	Grado de Accesibilidad
Rho de Spearman	Grado de Confidencialidad	Coeficiente de correlación	1,000	,436**
		Sig. (bilateral)	.	,005
		N	40	40
	Grado de Accesibilidad	Coeficiente de correlación	,436**	1,000
		Sig. (bilateral)	,005	.
		N	40	40

**. La correlación es significativa en el nivel 0,01 (bilateral).

(**Fuente**: elaboración propia)

Tabla 34: Tabla de correlación No paramétrica usando la prueba de correlación de Pearson entre las variables Confidencialidad y Accesibilidad.

Correlaciones

		Grado de Confidencialidad	Grado de Accesibilidad
Grado de Confidencialidad	Correlación de Pearson	1	,568**
	Sig. (bilateral)		,000
	N	40	40
Grado de Accesibilidad	Correlación de Pearson	,568**	1
	Sig. (bilateral)	,000	
	N	40	40

**. La correlación es significativa en el nivel 0,01 (bilateral).

(**Fuente**: elaboración propia)

Según los resultados del programa para la pruebas de correlación nos arrojan un 43.6% y 56.8% para Rho de Spearman y Pearson respectivamente. Siendo un grado de relación significante entre las variables por lo que podemos ir concluyendo que ambas variables están relacionadas positivamente a un 56.8%.

Deducción de correlación para C3: *La Accesibilidad tiene una influencia positiva sobre la Confidencialidad.*

Según los resultados hasta el momento se demuestra según la prueba chi-cuadrado que las variables Accesibilidad y Confidencialidad están relacionadas y con la prueba de Pearson demostramos que están correlacionas un 56.8% positivamente por lo que según nuestro objetivo de Implementar un modelo de buenas prácticas aplicando la Norma ISO 27002 para mejorar la gestión de incidencias de la red Wncor nos enfocaremos según nuestro modelo a buscar normas la cual nos ayuden a aumentar el grado de accesibilidad de los usuarios para buscar atacar de manera indirecta el grado de confidencialidad que estas deberían tener y así generar menor número de incidencias por el problema latente.

IMPLEMENTACIÓN DE RESULTADOS

"Aplicación de los controles de la Norma ISO 27002 según el modelo planteado en la tesis para la reducción de incidencias en la red Wncor."

La estrategia de mejorar la gestión de incidencias de la Red Wncor con el fin de reducir los incidentes presentados con los problemas de red nos llevó a plantear un modelo el cual podamos optimizar el uso de los controles que nos proporciona la Norma ISO 27002 con el objetivo de aplicarlas enfocándonos en el problema principal que se planteada en esta tesis. De esta forma buscaremos los controles más óptimos que nos ayudaran a mejorar la gestión de incidentes según nuestras variables planteadas relacionadas.

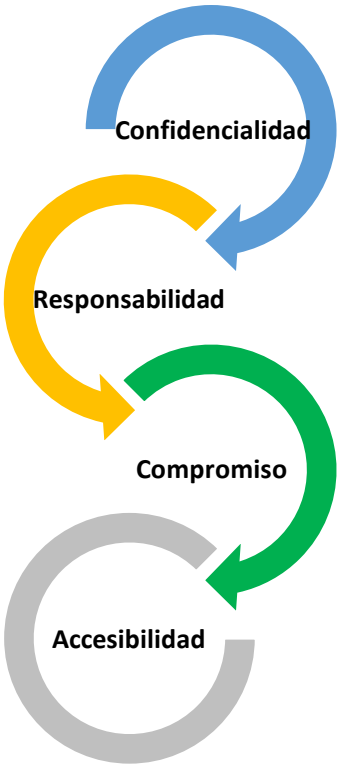


Figura 18: Dimensiones del modelo.

Hacemos mención que La norma ISO 27002:2013 contiene 14 dominios, 35 objetivos de control y 114 controles las cuales las correlacionaremos con nuestro modelo planteado y aplicamos los controles de acuerdo a la norma y nuestra variable realizamos

Confidencialidad:

Según Caccuri (2012), "debe tener la capacidad de proteger la Información ante el intento de acceso de divulgación a otros usuarios no autorizados. Consiste en asegurar la privacidad de los datos. Solamente los individuos, procesos o dispositivos autorizados pueden acceder a ellos".

Responsabilidad:

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva. Todos los usuarios deben ser conscientes de sus responsabilidades durante el mantenimiento de controles de acceso eficientes, en particular respecto a la utilización de las contraseñas y la seguridad en los equipos puestos en su disposición.

Accesibilidad

Grado en el que los usuarios pueden acceder a un servicio, independientemente de sus capacidades técnicas. Para promover la accesibilidad se hace uso de ciertas facilidades que ayudan a salvar los obstáculos o barreras de accesibilidad del entorno. Estas facilidades son llamadas ayudas técnicas.

- **Confidencialidad**

1. Requisitos de negocio para el control de Accesos

   Únicamente se debería proporcionar a los usuarios el acceso a las redes y a los servicios de red para cuyo uso hayan sido específicamente autorizados

2. Gestión de accesos de usuarios

   Debería implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.

3. Gestión de privilegios de acceso

   La asignación y el uso de privilegios de accesos deberían estar restringida y controlada.

4. Provisión de acceso de usuario

   Debería implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios

- **Responsabilidad**

5. Responsabilidad del usuario

   Se debería requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

6. Control de acceso a sistemas y aplicaciones

   Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debería controlar por medio de un procedimiento seguro de inicio de sesión.

   Los sistemas para la gestión de contraseñas deberían ser interactivos y establecer contraseñas seguras y robustas.

   Se debería restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.

7. Seguridad de las operaciones

   Se debería supervisar y ajustar la utilización de los recursos.

8. Separación de los recursos de desarrollo, prueba y operación.

   Deberían separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios en producción.

9. Registros y Supervisión

   Los dispositivos de registro y la información del registro deberían estar protegidos contra manipulaciones indebidas y accesos no autorizados.

10. Gestión del a vulnerabilidad técnica

    Se deberían establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.

- **Accesibilidad**

11. Controles de Red

    Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

12. Políticas y procedimientos de intercambio de información

    Deberían establecer políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

13. Gestionar el acceso físico a los activos de TI

    Implementa y define procedimientos para limitar, conceder y anular el acceso a edificios, áreas, locales, de acuerdo a las necesidades del negocio, incluyendo emergencias.

14. Gestionar la seguridad de los puestos de usuario final

    Garantiza que los puestos de usuario final (se puede decir, equipo sobremesa, portátil, servidor y otros equipos, softwares móviles y de red) estén salvaguardados a un nivel que es mayor o igual al que se encuentra definido en los requerimientos de seguridad de la información almacenada, transmitida o procesada.

15. Gestionar la seguridad de la red y las conexiones

    Emplea medidas de seguridad, además de procedimientos de gestión que estén relacionados para la protección de la información en cada uno de los modos de conexión.

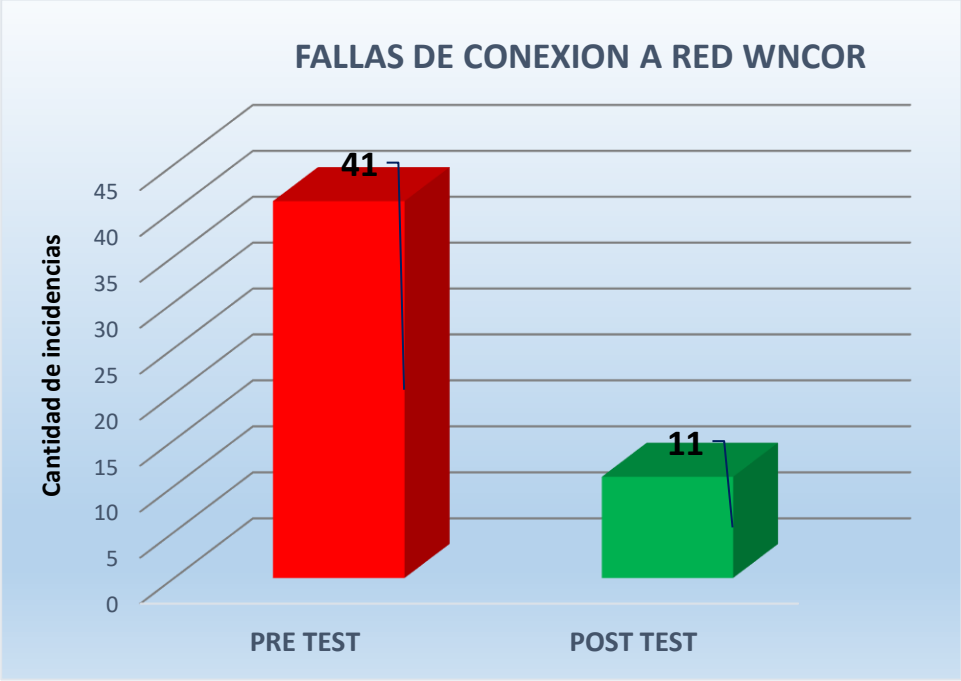
ANÁLISIS DESCRIPTIVOS DE LOS RESULTADOS

En el estudio se aplicó las buenas prácticas utilizando la Norma ISO 27002 para evaluar de qué manera esta norma nos ayuda con la gestión de incidencias y a la vez reduce las incidencias de fallas de conexión a la Red Wncor y los fallos de ingreso a los File Server; para ello se recolectó información del sistema CA Service Desk **(Anexo 3)** para obtener un Pre Test con la finalidad de conocer las condiciones iniciales de cada indicador, posteriormente se aplicaron las buenas practicas que brinda la Norma ISO 27002 que pudieron ser seleccionadas gracias al estudio de correlación entre: confidencialidad, responsabilidad, compromiso y accesibilidad. Aplicado todo el estudio en los usuarios de Interbank se volvió a recolectar los datos del mismo sistema CA Service Desk para obtener el Post Test.

INDICADOR: Fallas de conexión a la red Wncor

Los resultados del indicador Fallas de ingreso a la red Wncor se muestran en la figura N° 19

Para el caso del indicador de Fallas de ingreso a la Red Wncor, en el Pre-test de la muestra se obtuvo 41 incidencias registradas en el mes de Marzo, mientras que en el Post-test se tuvo sólo 11 incidentes registrados en el mes de Abril, esto muestra que existe una clara diferencia entre antes y después de la aplicación de buenas prácticas de la norma ISO 27002.



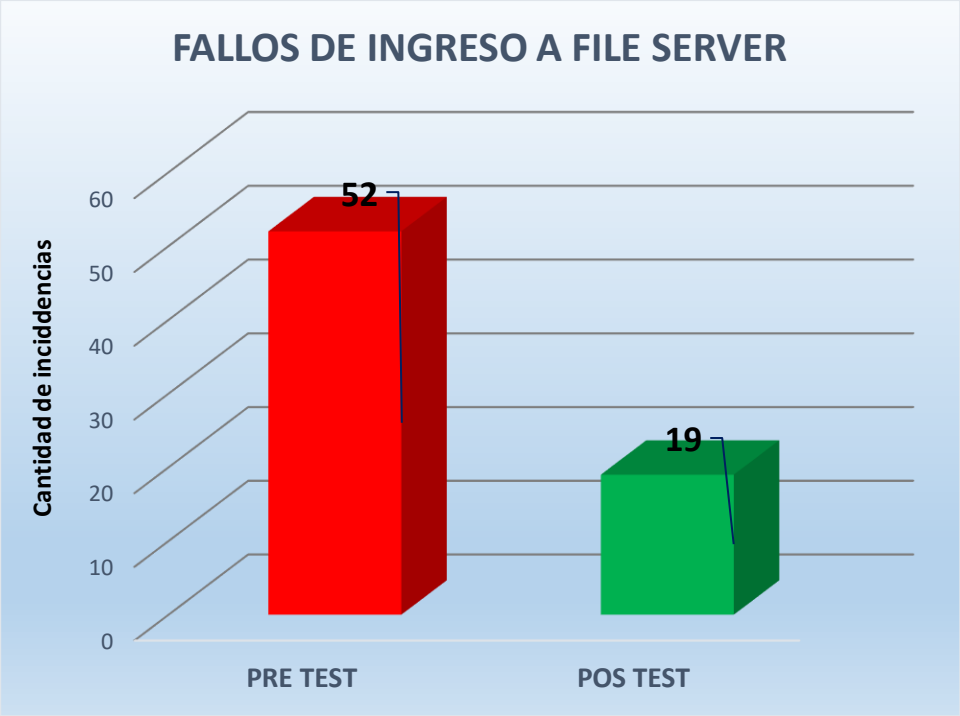
Fuente: Elaboración Propia

Figura 19: Indicador Fallas de conexión a red Wncor antes y después de la aplicación de la Norma ISO 27002.

INDICADOR: Fallos de ingresos a File Server

Los resultados del indicador Fallas de ingreso a File Server se muestran en la figura N° 20

Para el caso del indicador de Fallas de ingreso a File Server, en el Pre-test de la muestra se obtuvo 52 incidencias registradas en el mes de Marzo, mientras que en el Post-test se tuvo sólo 19 incidentes registrados en el mes de Abril, esto muestra que existe una clara diferencia entre antes y después de la aplicación de buenas prácticas de la norma ISO 27002.



Fuente: Elaboración Propia

Figura 20: Indicador Fallas de ingreso a File Server antes y después de la aplicación de la Norma ISO 27002.

PRUEBA DE HIPÓTESIS

Hipótesis General

$\boldsymbol{H_0}$: La Implementación del modelo de buenas prácticas aplicando ISO 27002 no mejora la gestión de incidencias de la red Wncor.

$\boldsymbol{H_1}$: La Implementación del modelo de buenas prácticas aplicando ISO 27002 mejora la gestión de incidencias de la red Wncor.

Tabla 35: Prueba de Rangos con signos de Wilcoxon.

Para el estudio de usuarios con incidentes en la red Wncor antes y después de la implementación de las buenas prácticas según la norma ISO 27002 para el modelo planteado.

Estadísticos de prueba[a]

	H1_despues_Prob_red_wncor - H1_antes_Prob_red_wncor
Z	-5,831[b]
Sig. asintótica (bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

(**Fuente**: elaboración propia)

De la **tabla N° 35**, se evaluó la significancia a sintónica (bilateral), donde se observa que la significancia estadística es de .000055, lo cual es <0.005, por lo que podemos afirmar que hay diferencias estadísticamente significativas entre las muestras relacionales (Pre-Test y Pos-Test), por lo que se rechaza la hipótesis nula y se acepta la hipótesis alterna (H1) donde indica que la implementación del modelo de buenas prácticas aplicando ISO 27002 mejora la gestión de incidencias de la red Wncor.

Hipótesis Específica 1

$\boldsymbol{H_0}$: El modelo de buenas prácticas aplicando ISO 27002 no reduce los problemas de conexión de la red Wncor.

$\boldsymbol{H_1}$: El modelo de buenas prácticas aplicando ISO 27002 reducirá los problemas de conexión de la red Wncor.

Tabla 36: Prueba de Rangos con signos de Wilcoxon.

Para el estudio de usuarios con incidentes de conexión en la red wncor antes y después de la implementación de las buenas prácticas según la norma ISO 27002 para el modelo planteado.

Estadísticos de prueba[a]

	H2_despues_conexion_red_wncor - H2_antes_conexion_red_wncor
Z	-5,657[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

(**Fuente**: elaboración propia)

De la **tabla N° 36**, se evaluó la significancia a sintónica (bilateral), donde se observa que la significancia estadística es de .000154, lo cual es <0.005, por lo que podemos afirmar que hay diferencias estadísticamente significativas entre las muestras relacionales (Pre-Test y Pos-Test), por lo que se rechaza la hipótesis nula y se acepta la hipótesis alterna (H1) donde indica el modelo de buenas prácticas aplicando ISO 27002 reducirá los problemas de conexión de la red Wncor.

Hipótesis Específica 2

$\boldsymbol{H_0}$: El modelo de buenas prácticas aplicando ISO 27002 no reduce los problemas de ingreso a los file server de la red Wncor.

$\boldsymbol{H_1}$: El modelo de buenas prácticas aplicando ISO 27002 reducirá los problemas de ingreso a los file server de la red Wncor.

Tabla 37: Prueba de Rangos con signos de Wilcoxon.

Para el estudio de usuarios con incidentes de ingreso a los file server de la red wncor antes y después de la implementación de las buenas prácticas según la norma ISO 27002 para el modelo planteado.

Estadísticos de prueba[a]

	H3_despues_fileserver_red_wncor - H3_antes_fileserver_red_wncor
Z	-5,396[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

(**Fuente**: elaboración propia)

De la **tabla N° 37**, se evaluó la significancia a sintónica (bilateral), donde se observa que la significancia estadística es de .000680, lo cual es <0.005, por lo que podemos afirmar que hay diferencias estadísticamente significativas entre las muestras relacionales (Pre-Test y Pos-Test), por lo que se rechaza la hipótesis nula y se acepta la hipótesis alterna (H2) donde indica el modelo de buenas prácticas aplicando ISO 27002 reducirá los problemas de ingreso a los file server de la red Wncor.

CAPITULO V:
DISCUSIÓN DE RESULTADOS

Discusión de resultados

- De acuerdo a lo demostrado aplicando el Modelo propuesto en la tesis para aplicar de forma óptima los controles de la norma ISO 27002 adecuados para mejorar la gestión de incidencias de red Wncor se concluye que la implementación del modelo de buenas prácticas aplicando ISO 27002 mejora la gestión de incidencias de la red Wncor llevando a más del 85% de usuarios con estos problemas a no tenerlos más.

- Se concluye que el modelo de buenas prácticas aplicando ISO 27002 reduce un 80% los problemas de conexión de la red Wncor en los usuarios estudiados.

- Se concluye que el modelo de buenas prácticas aplicando ISO 27002 reduce un 86% los problemas de ingreso a los file server de la red Wncor en los usuarios estudiados.

CONCLUSIONES:

1. Después de analizar las cuatro dimensiones como son: confidencialidad, Responsabilidad, Compromiso y accesibilidad hemos probado que el modelo para mejorar la Gestión de incidencias de red Wncor se basa en aplicar determinados roles de la norma ISO 27002 aplicando políticas de Roles de accesos, gestión de activos y reglas de seguridad. Esto en base a nuestras dimensiones hemos optimizado y aplicado el modelo donde se demuestra que *La implementación del modelo de buenas prácticas aplicando ISO 27002 mejora la gestión de incidencias de la red Wncor* principalmente mejorando y atacando las variables de responsabilidad, confidencialidad y compromiso.

2. Al aplicar el modelo de buenas prácticas de la norma ISO 27002 y seleccionando los controles adecuados según el modelo planteado en cuanto a las dimensiones probadas aplicadas a los 40 encuestados y en un estudio promedio de 4 semanas de implementarla impacta directamente reduciendo los problemas de conexión de la red Wncor.

3. Al aplicar el modelo de buenas prácticas de la norma ISO 27002 y seleccionando los controles adecuados según el modelo planteado en cuanto a las dimensiones probadas aplicadas a los 40 encuestados y en un estudio de 4 semanas de implementarla impacta directamente reduciendo los problemas de ingreso a los file server de la red Wncor.

RECOMENDACIONES:

1. Se recomienda realizar un análisis del estado situacional de incidencias en cuanto a problemáticas relacionadas a seguridad de información para detectar de manera más oportuna fraudes y malicias externas que puedan afectar la alta disponibilidad del banco.

2. Se recomienda realizar cursos y charlas informáticas con mayor frecuencia mediante videos online y presenciales explicando los controles más importantes de la Norma ISO 27002 para mejorar el grado de vulnerabilidad de las áreas más pequeñas.

3. Se recomienda brindar capacitaciones dinámicas tanto a colaboradores internos como externos para tener la seguridad que sobre resguardan la disponibilidad del banco ante posibles amenazas.

4. Por último, se recomienda a la empresa establecer como prioridad la certificación internacional de la norma ISO 27001, a los especialistas informáticos encargados con la implementación de la misma en sus respectivas áreas, con el fin de priorizar la Seguridad de la Información en las dependencias de las diferentes áreas del Banco.

REFERENCIAS BIBLIOGRAFICAS

BIBLIOGRAFIA

1. Daniel R. y Joffre V. Análisis e implementación de la Norma ISO 27002 para el departamento de sistemas de la universidad Politécnica Salesiana de la Sede Guayaquil". Tesis, Guayaquil, Ecuador; 2014. Ultimo ingreso; Jueves 7 de febrero del 2019.
2. Samuel G y Luis T. Implementación de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte. Tesis, Lima, Perú; 2018. Ultimo ingreso; Jueves 7 de febrero del 2019.
3. Roberto E. Implementación de la norma ISO/IEC 27002:2013, sección control de acceso para las aplicaciones informáticas de la aseguradora del sur. Tesis, Universidad de las Américas, Lima; Perú; 2014. Ultimo ingreso; Sábado 9 de febrero del 2019.
4. Miguel L. Diseño de los procesos de gestión de incidencias y service desk, alineado a las buenas prácticas de itil, aplicado a la empresa delltex industrial S.A. Tesis, Pontífica Universidad Católica del Ecuador, Quito; Ecuador. Ultimo ingreso; Martes 12 de febrero del 2019.
5. Benjy H. Sistema web para gestión de incidencias de la empresa CSD Electrónica SAC. Tesis, Universidad Cesar Vallejo, Lima; Perú; 2017. Ultimo ingreso; Domingo 17 de febrero del 2019.
6. Norma ISO 270002, Blog especializado en Sistemas de Gestión de Seguridad de la Información
   https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/
   Ultimo ingreso; Miércoles 13 de febrero del 2019

7. Gestión de Incidencias, Service Tonic
   https://www.servicetonic.es/itil/itil-v3-gestion-de-incidencias/
   Ultimo ingreso; Miércoles 13 de febrero del 2019

8. Gestión de Incidencias, Wikipedia
https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_incidentes
Ultimo ingreso; Miércoles 13 de febrero del 2019

9. Métodos de investigación de enfoque experimental, UNE Enrique Guzmán y Valle
http://www.postgradoune.edu.pe/pdf/documentos-academicos/ciencias-de-la-educacion/10.pdf
Ultimo ingreso; Jueves 14 de febrero del 2019

10. SPSS, Wikipedia
https://es.wikipedia.org/wiki/SPSS
Ultimo ingreso; Domingo 17 de febrero del 2019

11. Prueba de Chi-cuadrado, IBM Knowledge Center IBM®
https://www.ibm.com/support/knowledgecenter/es/SSLVMB_sub/statistics_mainhelp_ddita/spss/base/idh_ntch.html
Ultimo ingreso; Domingo 17 de febrero del 2019

12. Chi cuadrado, SAMUIC
http://www.samiuc.es/estadisticas-variables-binarias/valoracion-inicial-pruebas-diagnosticas/chi-cuadrado/
Ultimo ingreso; Domingo 17 de febrero del 2019

13. Alfa de Cronbach
https://es.wikipedia.org/wiki/Alfa_de_Cronbach
Ultimo ingreso; Domingo 17 de febrero del 2019

14. Prueba de los rangos con signo de Wilcoxon
https://es.wikipedia.org/wiki/Prueba_de_los_rangos_con_signo_de_Wilcoxon
Ultimo ingreso; Domingo 17 de febrero del 2019

15. Coeficiente de correlación de Spearman
https://es.wikipedia.org/wiki/Coeficiente_de_correlaci%C3%B3n_de_Spearman
Ultimo ingreso; Domingo 17 de febrero del 2019

16. Coeficiente de Correlación Lineal de Person
https://personal.us.es/vararey/adatos2/correlacion.pdf
Ultimo ingreso; lunes 18 de febrero del 2019

17. Coeficiente de Correlación Lineal de Person
https://www.conevyt.org.mx/bachillerato/material_bachilleres/cb6/5sempdf/edin1/edi1_f03.pdf
Ultimo ingreso; Domingo 17 de febrero del 2019

18. Coeficiente de Correlación Rho de Spearman
Libro Estadística no Paramétrica – autor SidneySiegel – N. John Castellan
Ultimo ingreso; Domingo 17 de febrero del 2019

19. Análisis de Fiabilidad
https://upcommons.upc.edu/bitstream/handle/2117/76844/JENUI2015_146-153.pdf
Ultimo ingreso; Domingo 17 de febrero del 2019

20. Modelo de Regresión Lineal
http://www.dm.uba.ar/materias/estadistica_Q/2011/1/clase%20regresion%20simple.pdf
Ultimo ingreso; Domingo 17 de febrero del 2019

ANEXOS

ANEXO 1: Instrumento de Ficha de Observación

A continuación, se muestra la ficha de observación aplicada para este trabajo de investigación incluyendo las dos dimensiones empleadas con sus respectivas métricas con información actual del pos test y el pre test.

FALLOS DE CONEXIÓN A RED WNCOR								
	PRETEST				POSTEST			
N°	N° de Ticket	Fecha de Apertura	Rango de Fechas	N° Total de Fallos	N° de Ticket	Fecha de Apertura	Rango de Fechas	N° Total de Fallos
1	2484144	30/03/2019 19:31	del 26/3/2019 al 31/3/2019	13	2507498	30/04/2019 14:05	del 26/4/2019 al 30/4/2019	2
2	2484137	30/03/2019 19:24			2507321	30/04/2019 12:09		
3	2484108	30/03/2019 19:01						
4	2472822	29/03/2019 17:32						
5	2472818	29/03/2019 17:28						
6	2477936	29/03/2019 10:54						
7	2468191	28/03/2019 14:35						
8	2457720	28/03/2019 09:34						
9	2457370	27/03/2019 17:50						
10	2452303	27/03/2019 00:12						
11	2328599	26/03/2019 09:38						
12	2451305	26/03/2019 06:46						
13	2474312	26/03/2019 06:34						
14	2473457	25/03/2019 11:39	del 21/3/2019 al 25/3/2019	5	2499794	23/04/2019 13:06	del 21/4/2019 al 25/4/2019	3
15	2434553	23/03/2019 15:42			2499741	23/04/2019 12:39		
16	2433733	22/03/2019 17:46			2498443	22/04/2019 14:28		
17	2496507	22/03/2019 01:09						
18	2424920	21/03/2019 18:22						
19	2447328	20/03/2019 12:06	del 16/3/2019	11			del 16/4/2019	0

20	2446750	19/03/2019 18:26	al 20/3/2019				al 20/4/2019	
21	2445262	18/03/2019 17:02						
22	2445136	18/03/2019 15:40						
23	2444520	18/03/2019 09:29						
24	2444426	18/03/2019 08:16						
25	2439819	15/03/2019 12:01	del 11/3/2019 al 15/3/2019		2493890	15/04/2019 15:17	del 11/4/2019 al 15/4/2019	3
26	2466177	15/03/2019 08:39			2493497	15/04/2019 11:32		
27	2431863	13/03/2019 12:02			2491804	12/04/2019 11:50		
28	2437636	11/03/2019 18:14						
29	2437228	11/03/2019 12:26						
30	2485423	09/03/2019 16:14	del 6/3/2019 al 10/3/2019	5			del 6/4/2019 al 10/4/2019	0
31	2466066	08/03/2019 14:43						
32	2431594	08/03/2019 08:31						
33	2431335	07/03/2019 18:41						
34	2464845	07/03/2019 12:24						
35	2428025	05/03/2019 19:32	del 1/3/2019 al 5/3/2019	7	2484303	04/04/2019 19:56	del 1/4/2019 al 5/4/2019	3
36	2427722	05/03/2019 15:49			2480187	01/04/2019 18:46		
37	2422550	05/03/2019 15:25			2479832	01/04/2019 15:36		
38	2412818	04/03/2019 17:56						
39	2412791	03/03/2019 17:35						
40	2402550	02/03/2019 15:25						
41	2138766	01/03/2019 07:29						

FALLOS DE INGRESO A FILE SERVER

	PRETEST				POSTEST			
N°	N° de Ticket	Fecha de Apertura	Rango de Fechas	N° Total de Fallos	N° de Ticket	Fecha de Apertura	Rango de Fechas	N° Total de Fallos
1	2477972	29/03/2019 11:16	del 26/3/2019 al 31/3/2019	7	2506031	29/04/2019 16:41	del 26/4/2019 al 31/4/2019	2
2	2477728	29/03/2019 08:10			2504168	26/04/2019 16:26		
3	2454233	28/03/2019 17:18						
4	2477409	28/03/2019 16:33						
5	2454058	28/03/2019 14:46						
6	2476896	28/03/2019 10:20						
7	2453658	28/03/2019 09:55						
8	2474113	25/03/2019 18:23	del 21/3/2019 al 25/3/2019	7	2502502	25/04/2019 11:19	del 21/4/2019 al 25/4/2019	3
9	2474077	25/03/2019 17:53			2501244	24/04/2019 12:21		
10	2450912	25/03/2019 16:20			2499048	23/04/2019 08:13		
11	2450690	25/03/2019 12:58						
12	2449994	23/03/2019 13:03						
13	2449527	22/03/2019 14:21						
14	2448437	21/03/2019 12:29						
15	2470735	20/03/2019 21:40	del 16/3/2019 al 20/3/2019	4	2496686	17/04/2019 17:49	del 16/4/2019 al 20/4/2019	3
16	2446920	20/03/2019 06:30			2496539	17/04/2019 16:11		
17	2446165	19/03/2019 12:19			2496159	17/04/2019 11:47		
18	2468359	18/03/2019 19:52						
19	2466290	15/03/2019 09:49	del 11/3/2019 al 15/3/2019	13	2494331	15/04/2019 19:11	del 11/4/2019 al 15/4/2019	2
20	2443453	15/03/2019 09:30			2491230	11/04/2019 23:10		
21	2464191	13/03/2019 10:30						
22	2442280	13/03/2019 17:59						
23	2442090	13/03/2019 15:36						

24	2463847	12/03/2019 19:00						
25	2463640	12/03/2019 16:36						
26	2463577	12/03/2019 16:02						
27	2440998	12/03/2019 12:55						
28	2440953	12/03/2019 11:58						
29	2440085	11/03/2019 12:40						
30	2462236	11/03/2019 14:40						
31	2461889	11/03/2019 10:55						
32	2460899	08/03/2019 15:42	del 6/3/2019 al 10/3/2019	12	2489329	10/04/2019 13:48	del 6/4/2019 al 10/4/2019	3
33	2459974	07/03/2019 16:56			2489313	10/04/2019 13:30		
34	2438356	07/03/2019 17:58			2488228	09/04/2019 15:42		
35	2438086	07/03/2019 14:48						
36	2437517	07/03/2019 00:23						
37	2437515	07/03/2019 00:17						
38	2459170	06/03/2019 22:37						
39	2458818	06/03/2019 15:49						
40	2458343	06/03/2019 10:07						
41	2458303	06/03/2019 09:38						
42	2437094	06/03/2019 15:20						
43	2437077	06/03/2019 14:59			2487124	08/04/2019 17:57		
44	2436420	05/03/2019 18:29	del 1/3/2019 al 5/3/2019	9	2482188	03/04/2019 11:06	del 1/4/2019 al 5/4/2019	6
45	2436195	05/03/2019 15:55			2481963	03/04/2019 09:28		
46	2435734	05/03/2019 09:45			2481660	02/04/2019 19:09		
47	2435186	04/03/2019 15:11			2481507	02/04/2019 17:34		
48	2434457	03/03/2019 02:55			2479845	01/04/2019 15:46		
49	2434366	02/03/2019 12:48			2479504	01/04/2019 12:04		
50	2425100	01/03/2019 14:58						

51	2425099	01/03/2019 14:57						
52	2424946	01/03/2019 12:36						

ANEXO 2: Validación de instrumento - ficha de observación

VALIDACION DE INSTRUMENTO – FICHA DE EXPERTO: FALLOS DE CONEXIÓN A RED WNCOR

VALIDACION DE INSTRUMENTOS

I. DATOS GENERALES

1.1. Apellidos y Nombres del Experto: LOLIWELD ZEGARRA, MANUEL

1.2. Cargo e Institución donde Labora: DOCENTE.
Universidad Peruana Los Andes, Escuela Académica Profesional de Ingeniería de Sistemas y computación

1.3. Nombre del Instrumento motivo de Evaluación:
Ficha de Experto – FALLOS DE CONEXIÓN A RED WNCOR

1.4. Título de la investigación:
Modelo de buenas prácticas aplicando ISO 27002 para la gestión de incidencias de la red Wncor.

1.5. Autor:
Ledy Ruth Sandoval Fernández

II. ASPECTOS DE VALIDACION

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50%	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
1 CLARIDAD	Está formado con el lenguaje apropiado				78	
2 OBJETIVIDAD	Está expresado en conducta observable				75	
3 ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología				80	
4 ORGANIZACION	Existe una organización lógica				78	
5 SUFICIENCIA	Comprende los aspecto de cantidad y claridad				80	
6 INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico				80	
7 CONSISTENCIA	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa				80	
8 COHERENCIA	Entre los índices, indicadores, dimensiones				75	
9 METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr				78	
10 PERTINENCIA	El instrumento es adecuado al tipo de investigación				80	
PROMEDIO DE VALIDACIÓN						

III. PROMEDIO DE VALIDACIÓN: 78.4%

IV. OPCION DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado.
( ) El instrumento debe ser mejorado antes de ser aplicado.
En caso el instrumento no deba ser aplicado por favor justifique su opinión

Fecha: 17/05/2019

Firma del experto

VALIDACION DE INSTRUMENTO – JUICIO DE EXPERTO: FALLOS DE INGRESO A FILE SERVER

VALIDACION DE INSTRUMENTOS

I. DATOS GENERALES

1.1. Apellidos y Nombres del Experto: VALENTIN TEODORO DIAZ CHU

1.2. Cargo e Institución donde Labora: DOCENTE
Universidad Peruana Los Andes, Escuela Académica Profesional de Ingeniería de Sistemas y computación

1.3. Nombre del Instrumento motivo de Evaluación:
Ficha de Experto – FALLOS DE INGRESO A FILE SERVER

1.4. Título de la investigación:
Modelo de buenas prácticas aplicando ISO 27002 para la gestión de incidencias de la red Wncor.

1.5. Autor:
Ledy Ruth Sandoval Fernández

II. ASPECTOS DE VALIDACION

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50%	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
1 CLARIDAD	Está formado con el lenguaje apropiado				80	
2 OBJETIVIDAD	Está expresado en conducta observable				75	
3 ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología				80	
4 ORGANIZACION	Existe una organización lógica				80	
5 SUFICIENCIA	Comprende los aspecto de cantidad y claridad				75	
6 INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico				80	
7 CONSISTENCIA	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa				80	
8 COHERENCIA	Entre los índices, indicadores, dimensiones				78	
9 METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr				80	
10 PERTINENCIA	El instrumento es adecuado al tipo de investigación				80	
PROMEDIO DE VALIDACIÓN						

III. PROMEDIO DE VALIDACIÓN: 78.8%

IV. OPCION DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado.
( ) El instrumento debe ser mejorado antes de ser aplicado.

En caso el instrumento no deba ser aplicado por favor justifique su opinión

Fecha: 17/05/2019

Firma del experto

VALIDACION DE INSTRUMENTO – FICHA DE EXPERTO: FALLOS DE CONEXIÓN A RED WNCOR

VALIDACION DE INSTRUMENTOS

I. DATOS GENERALES

1.1. Apellidos y Nombres del Experto: Carla Santivañez Calderon

1.2. Cargo e Institución donde Labora:
Universidad Peruana Los Andes, Escuela Académica Profesional de Ingeniería de Sistemas y computación

1.3. Nombre del Instrumento motivo de Evaluación:
Ficha de Experto – FALLOS DE CONEXIÓN A RED WNCOR

1.4. Título de la investigación:
Modelo de buenas prácticas aplicando ISO 27002 para la gestión de incidencias de la red Wncor.

1.5. Autor:
Ledy Ruth Sandoval Fernández

II. ASPECTOS DE VALIDACION

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50%	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
1 CLARIDAD	Está formado con el lenguaje apropiado				75%	
2 OBJETIVIDAD	Está expresado en conducta observable				72%	
3 ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					83%
4 ORGANIZACION	Existe una organización lógica				75%	
5 SUFICIENCIA	Comprende los aspecto de cantidad y claridad				78%	
6 INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					84%
7 CONSISTENCIA	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa				76%	
8 COHERENCIA	Entre los índices, indicadores, dimensiones				80%	
9 METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr					82%
10 PERTINENCIA	El instrumento es adecuado al tipo de investigación				80%	
PROMEDIO DE VALIDACIÓN						

III. PROMEDIO DE VALIDACIÓN: 78.5%

IV. OPCION DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado.
( ) El instrumento debe ser mejorado antes de ser aplicado.

En caso el instrumento no deba ser aplicado por favor justifique su opinión

Fecha: 17/05/2019

Firma del experto

Carla María Santivañez Calderón
Maestra en Docencia Superior e Investigación
INGENIERA DE SISTEMAS
CIP 158188

VALIDACION DE INSTRUMENTO – JUICIO DE EXPERTO: FALLOS DE INGRESO A FILE SERVER

VALIDACION DE INSTRUMENTOS

I. DATOS GENERALES

1.1. **Apellidos y Nombres del Experto:** Carla Santivañez Calderon

1.2. **Cargo e Institución donde Labora:**
Universidad Peruana Los Andes, Escuela Académica Profesional de Ingeniería de Sistemas y computación

1.3. **Nombre del Instrumento motivo de Evaluación:**
Ficha de Experto – FALLOS DE INGRESO A FILE SERVER

1.4. **Título de la investigación:**
Modelo de buenas prácticas aplicando ISO 27002 para la gestión de incidencias de la red Wncor.

1.5. **Autor:**
Ledy Ruth Sandoval Fernández

II. ASPECTOS DE VALIDACION

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50%	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
1 CLARIDAD	Está formado con el lenguaje apropiado				73%	
2 OBJETIVIDAD	Está expresado en conducta observable				78%	
3 ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología				80%	
4 ORGANIZACION	Existe una organización lógica					83%
5 SUFICIENCIA	Comprende los aspecto de cantidad y claridad				76%	
6 INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					82%
7 CONSISTENCIA	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa				78%	
8 COHERENCIA	Entre los índices, indicadores, dimensiones				80%	
9 METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr					83%
10 PERTINENCIA	El instrumento es adecuado al tipo de investigación				75%.	
PROMEDIO DE VALIDACIÓN						

III. **PROMEDIO DE VALIDACIÓN:** 78-8%

IV. **OPCION DE APLICABILIDAD**

(X) El instrumento puede ser aplicado, tal como está elaborado.
( ) El instrumento debe ser mejorado antes de ser aplicado.
En caso el instrumento no deba ser aplicado por favor justifique su opinión

Fecha: 17/05/2019

Firma del experto

Carla María Santivañez Calderón
Maestra en Docencia Superior e Investigación
INGENIERA DE SISTEMAS
CIP 158188

VALIDACION DE INSTRUMENTO – FICHA DE EXPERTO: FALLOS DE CONEXIÓN A RED WNCOR

VALIDACION DE INSTRUMENTOS

I. DATOS GENERALES

1.1. Apellidos y Nombres del Experto: BLAS REBAZA, MARUJA

1.2. Cargo e Institución donde Labora:
Universidad Peruana Los Andes, Escuela Académica Profesional de Ingeniería de Sistemas y computación

1.3. Nombre del Instrumento motivo de Evaluación:
Ficha de Experto – FALLOS DE CONEXIÓN A RED WNCOR

1.4. Título de la investigación:
Modelo de buenas prácticas aplicando ISO 27002 para la gestión de incidencias de la red Wncor.

1.5. Autor:
Ledy Ruth Sandoval Fernández

II. ASPECTOS DE VALIDACION

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50%	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
1 CLARIDAD	Está formado con el lenguaje apropiado				73%	
2 OBJETIVIDAD	Está expresado en conducta observable				75%	
3 ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología				80%	
4 ORGANIZACION	Existe una organización lógica				78%	
5 SUFICIENCIA	Comprende los aspecto de cantidad y claridad				76%	
6 INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico				72%	
7 CONSISTENCIA	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa				75%	
8 COHERENCIA	Entre los índices, indicadores, dimensiones				80%	
9 METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr				78	
10 PERTINENCIA	El instrumento es adecuado al tipo de investigación				80%	
PROMEDIO DE VALIDACIÓN						

III. PROMEDIO DE VALIDACIÓN: 76.7%

IV. OPCION DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado.
( ) El instrumento debe ser mejorado antes de ser aplicado.

En caso el instrumento no deba ser aplicado por favor justifique su opinión

Fecha: 20/05/2019

Firma del experto

VALIDACION DE INSTRUMENTO – JUICIO DE EXPERTO: FALLOS DE INGRESO A FILE SERVER

VALIDACION DE INSTRUMENTOS

I. DATOS GENERALES

1.1. Apellidos y Nombres del Experto: BLAS REBAZA, MARUJA

1.2. Cargo e Institución donde Labora:
Universidad Peruana Los Andes, Escuela Académica Profesional de Ingeniería de Sistemas y computación

1.3. Nombre del Instrumento motivo de Evaluación:
Ficha de Experto – FALLOS DE INGRESO A FILE SERVER

1.4. Título de la investigación:
Modelo de buenas prácticas aplicando ISO 27002 para la gestión de incidencias de la red Wncor.

1.5. Autor:
Ledy Ruth Sandoval Fernández

II. ASPECTOS DE VALIDACION

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50%	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
1 CLARIDAD	Está formado con el lenguaje apropiado				75 %	
2 OBJETIVIDAD	Está expresado en conducta observable				73%	
3 ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología				72%	
4 ORGANIZACION	Existe una organización lógica				78%	
5 SUFICIENCIA	Comprende los aspecto de cantidad y claridad				80%	
6 INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico				75%	
7 CONSISTENCIA	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa				78%	
8 COHERENCIA	Entre los índices, indicadores, dimensiones				80%	
9 METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr				73%	
10 PERTINENCIA	El instrumento es adecuado al tipo de investigación				80%	
PROMEDIO DE VALIDACION						

III. PROMEDIO DE VALIDACIÓN: 76.4%

IV. OPCION DE APLICABILIDAD

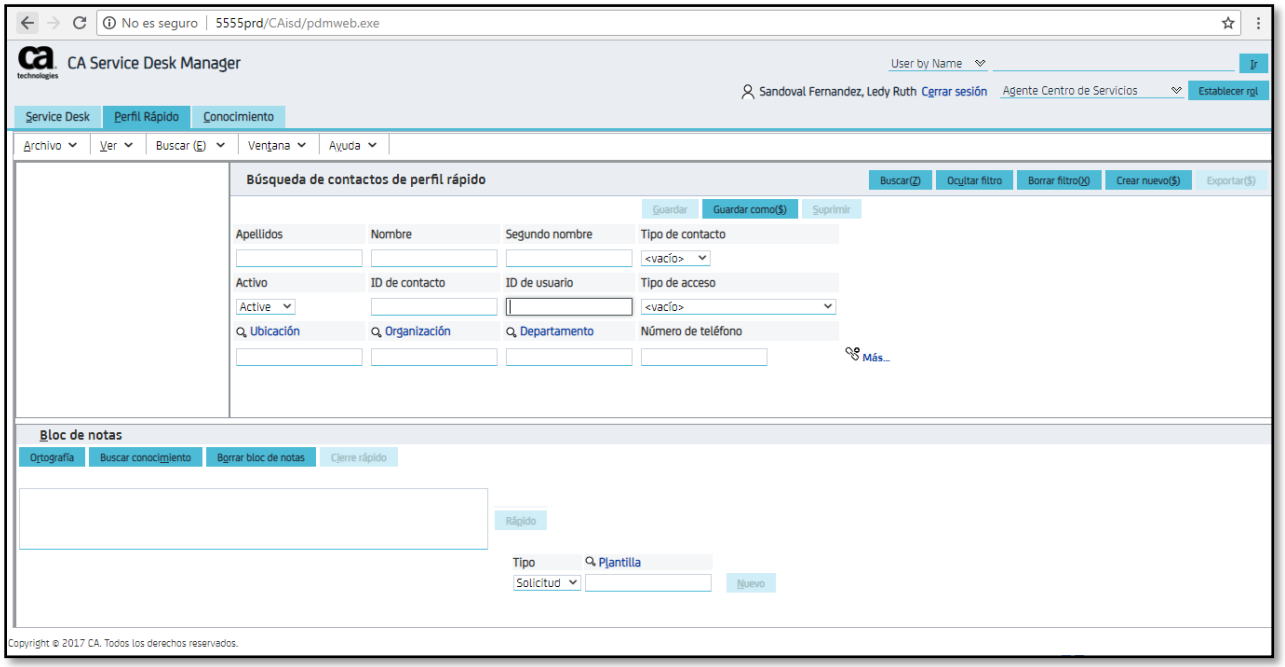
(X) El instrumento puede ser aplicado, tal como está elaborado.
( ) El instrumento debe ser mejorado antes de ser aplicado.

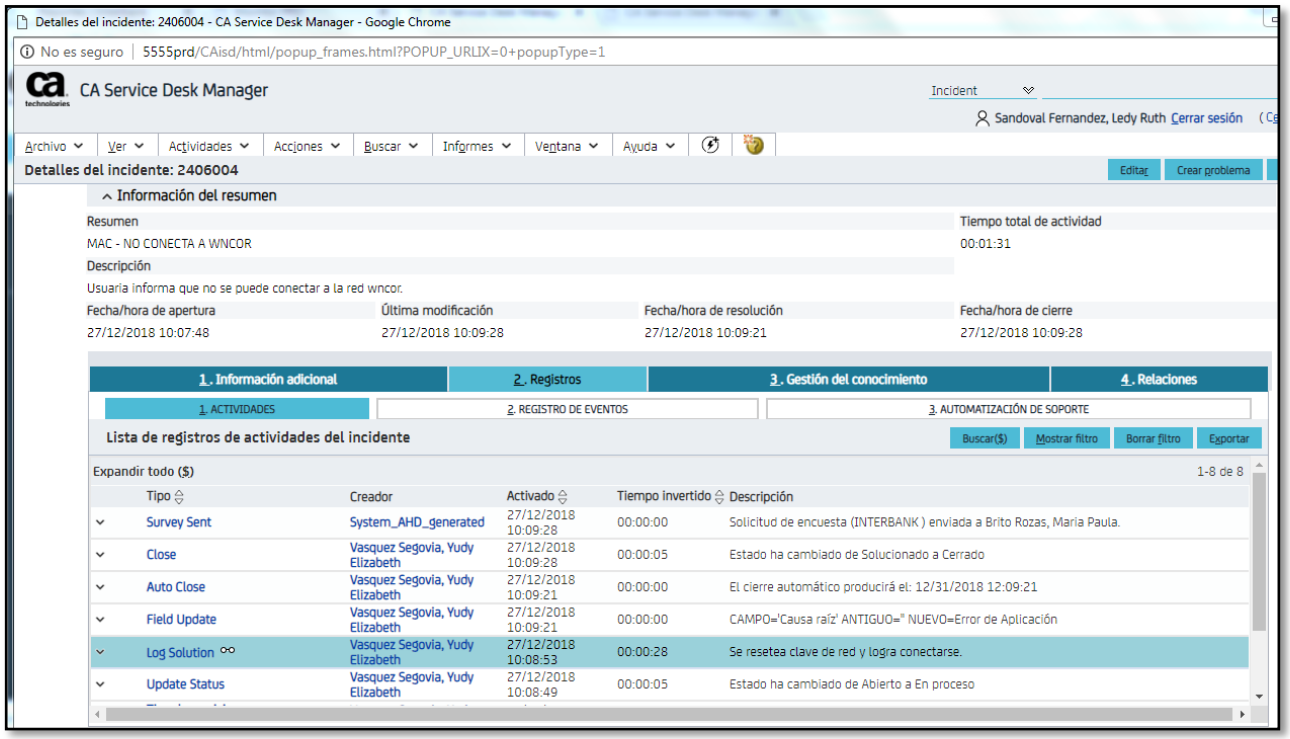
En caso el instrumento no deba ser aplicado por favor justifique su opinión

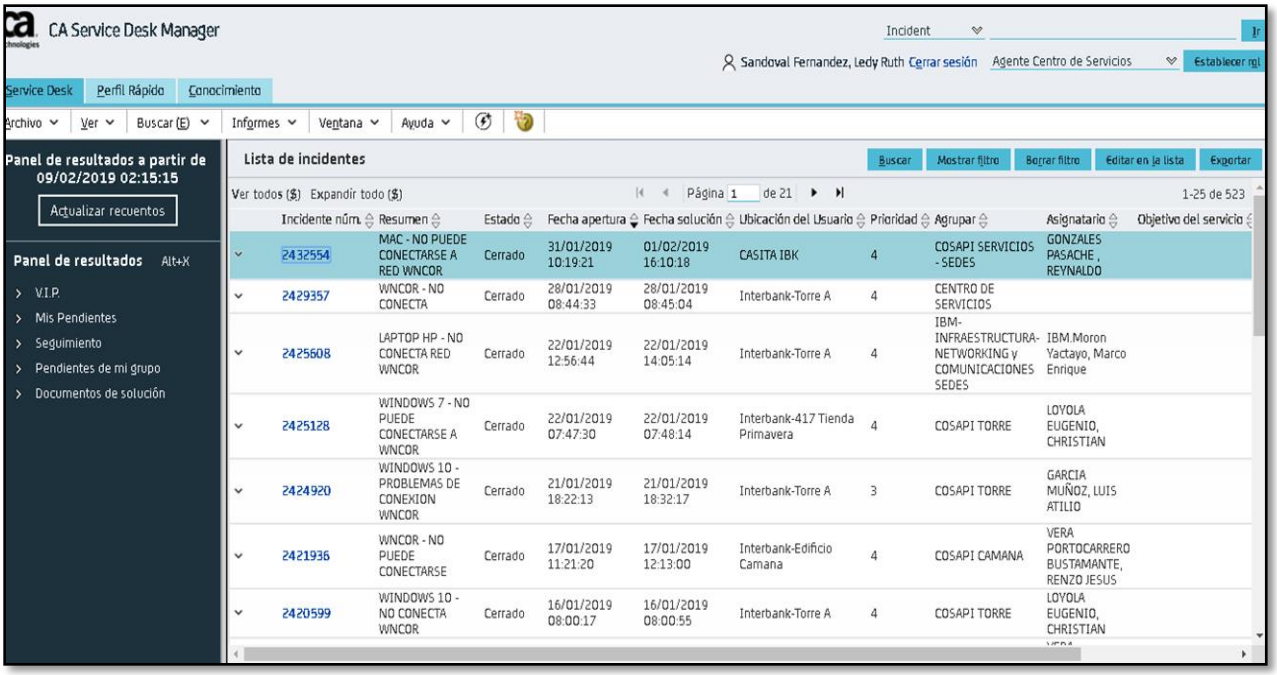
Fecha: 20/05/2019

Firma del experto
Mg. Maruja Blas Rebaza.

ANEXO 3: Programa ca service desk de donde se generan los tickes por incidencias presentadas de los usuarios






CA Service Desk Manager
Incident
Sandoval Fernandez, Ledy Ruth Cerrar sesión
Agente Centro de Servicios
Service Desk
Perfil Rápido
Conocimiento
Archivo
Ver
Buscar (E)
Informes
Ventana
Ayuda
Panel de resultados a partir de 09/02/2019 02:15:15
Actualizar recuentos
Panel de resultados Alt+X
V.I.P.
Mis Pendientes
Seguimiento
Pendientes de mi grupo
Documentos de solución
Lista de incidentes
Buscar
Mostrar filtro
Borrar filtro
Editar en la lista
Exportar
Ver todos ($) Expandir todo ($)
Página 1 de 21
1-25 de 523
Incidente núm.
Resumen
Estado
Fecha apertura
Fecha solución
Ubicación del Usuario
Prioridad
Agrupar
Asignatario
Objetivo del servicio
2432554 MAC - NO PUEDE CONECTARSE A RED WNCOR Cerrado 31/01/2019 10:19:21 01/02/2019 16:10:18 CASITA IBK 4 COSAPI SERVICIOS - SEDES GONZALES PASACHE , REYNALDO
2429357 WNCOR - NO CONECTA Cerrado 28/01/2019 08:44:33 28/01/2019 08:45:04 Interbank-Torre A 4 CENTRO DE SERVICIOS
2425608 LAPTOP HP - NO CONECTA RED WNCOR Cerrado 22/01/2019 12:56:44 22/01/2019 14:05:14 Interbank-Torre A 4 IBM-INFRAESTRUCTURA-NETWORKING y COMUNICACIONES SEDES IBM.Moron Yactayo, Marco Enrique
2425128 WINDOWS 7 - NO PUEDE CONECTARSE A WNCOR Cerrado 22/01/2019 07:47:30 22/01/2019 07:48:14 Interbank-417 Tienda Primavera 4 COSAPI TORRE LOYOLA EUGENIO, CHRISTIAN
2424920 WINDOWS 10 - PROBLEMAS DE CONEXION WNCOR Cerrado 21/01/2019 18:22:13 21/01/2019 18:32:17 Interbank-Torre A 3 COSAPI TORRE GARCIA MUÑOZ, LUIS ATILIO
2421936 WNCOR - NO PUEDE CONECTARSE Cerrado 17/01/2019 11:21:20 17/01/2019 12:13:00 Interbank-Edificio Camana 4 COSAPI CAMANA VERA PORTOCARRERO BUSTAMANTE, RENZO JESUS
2420599 WINDOWS 10 - NO CONECTA WNCOR Cerrado 16/01/2019 08:00:17 16/01/2019 08:00:55 Interbank-Torre A 4 COSAPI TORRE LOYOLA EUGENIO, CHRISTIAN

CUESTIONARIO

Modelo de buenas prácticas aplicando ISO 27002 para gestión de incidencias de la red Wncor.

OBJETIVO: Implementar un modelo de buenas prácticas aplicando ISO 27002 para mejorar la gestión de incidencias de la red Wncor.

INSTRUCCIONES: El presente cuestionario tiene como finalidad recoger datos para utilizarlo en la investigación cuyas respuestas serán anónimas y confidenciales, agradeciendo de antemano su participación.

Por favor marca con una (**X**) la respuesta que creas es correcta para ti de acuerdo a las preguntas.

PREGUNTAS	RESPUESTAS		
	SIEMPRE	**ALGUNAS VECES**	**NUNCA**
1. *¿Alguna vez has brindado tu clave de red a otro usuario?*			
2. *¿Bloqueas tu pc cuando sales de tu sitio?*			
3. *¿Prestaste tu equipo a otro usuario?*			
4. *¿Cierras la sesión de tu equipo al final del día?*			
5. *¿Le das importancia a las notificaciones de cambio de contraseña?*			
6. *¿Pides tú contraseña con opción a cambio al Centro De Servicios?*			
7. *¿Te desconectas de la Wncor cuando acabas tus actividades?*			
8. *¿Te quitaron el acceso a Wncor sin informarte?*			
9. *¿Estas al tanto de cuando expira tu cuenta de red?*			
10. *¿Cuándo pides tus accesos te lo dan a tiempo?*			
11. *¿Cambiaron tu clave de red sin tu autorización o consentimiento?*			
12. *¿Antes de conectar a Wncor te desconectas del cable red?*			
13. *¿Te has equivocado en utilizar la Wncor con la Wifree?*			

ANEXO 4: Validación de instrumento – encuesta

VALIDACION DE INSTRUMENTO – JUICIO DE EXPERTO: ENCUESTA

I. DATOS GENERALES

1.1. Apellidos y Nombres del Experto: VALENZUELA TEODORO, DANIELLO

1.2. Cargo e Institución donde Labora: DOCENTE
Universidad Peruana Los Andes, Escuela Académica Profesional de Ingeniería de Sistemas y computación

1.3. Nombre del Instrumento motivo de Evaluación:
Encuesta

1.4. Título de la investigación:
Modelo de buenas prácticas aplicando ISO 27002 para la gestión de incidencias de la red Wncor.

1.5. Autor:
Ledy Ruth Sandoval Fernández

II. ASPECTOS DE VALIDACION

0-20% = Deficiente 21-50% =Regular 51-70%= Bueno 71-80%= Muy Bueno 81-100%=Excelente

PREGUNTAS	Claridad en la redacción	Coherencia interna	Lenguaje adecuado	Nivel de entendimiento	Pertinente para los objetivos	Facilidad de comprensión	Inducción a la respuesta	TOTAL
	CALIFICACION DEL NIVEL DE ACEPTACION DE LAS PREGUNTAS							
P1								76
P2								80
P3								82
P4								75
P5								80
P6								85
P7								73
P8								80
P9								80
P10								75
P11								75
P12								82
P13								85
TOTAL DE RESULTADOS								1028
PROMEDIO DE VALIDACIÓN								79.07%

I. PROMEDIO DE VALIDACIÓN: 79.07%

II. OPCION DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado.
( ) El instrumento debe ser mejorado antes de ser aplicado.

En caso el instrumento no deba ser aplicado por favor justifique su opinión

Fecha: 05/03/2019

Firma del experto

VALIDACION DE INSTRUMENTO – JUICIO DE EXPERTO: ENCUESTA

I. DATOS GENERALES

1.1. Apellidos y Nombres del Experto: Carla Santivañez Calderon

1.2. Cargo e Institución donde Labora:
Universidad Peruana Los Andes, Escuela Académica Profesional de Ingeniería de Sistemas y computación

1.3. Nombre del Instrumento motivo de Evaluación:
Encuesta

1.4. Título de la investigación:
Modelo de buenas prácticas aplicando ISO 27002 para la gestión de incidencias de la red Wncor.

1.5. Autor:
Ledy Ruth Sandoval Fernández

II. ASPECTOS DE VALIDACION

0-20% = Deficiente 21-50% =Regular 51-70%= Bueno 71-80%= Muy Bueno 81-100%=Excelente

PREGUNTAS	Claridad en la redacción	Coherencia interna	Lenguaje adecuado	Nivel de entendimiento	Pertinente para los objetivos	Facilidad de comprensión	Inducción a la respuesta	TOTAL
	CALIFICACION DEL NIVEL DE ACEPTACION DE LAS PREGUNTAS							
P1								82%
P2								73%
P3								75%
P4								80%
P5								70%
P6								76%
P7								83%
P8								75%
P9								78%
P10								82%
P11								75%
P12								72%
P13								78%
TOTAL DE RESULTADOS								
PROMEDIO DE VALIDACIÓN								

I. PROMEDIO DE VALIDACIÓN: 76.84%

II. OPCION DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado.
( ) El instrumento debe ser mejorado antes de ser aplicado.

En caso el instrumento no deba ser aplicado por favor justifique su opinión

Fecha: 05/03/2019

Firma del experto

Carla María Santivañez Calderón
Maestra en Docencia Superior e Investigación
INGENIERA DE SISTEMAS
CIP 158188

VALIDACION DE INSTRUMENTO – JUICIO DE EXPERTO: ENCUESTA

I. DATOS GENERALES

1.1. Apellidos y Nombres del Experto: BLAS REBAZA, MARUJA

1.2. Cargo e Institución donde Labora:
Universidad Peruana Los Andes, Escuela Académica Profesional de Ingeniería de Sistemas y computación

1.3. Nombre del Instrumento motivo de Evaluación:
Encuesta

1.4. Título de la investigación:
Modelo de buenas prácticas aplicando ISO 27002 para la gestión de incidencias de la red Wncor.

1.5. Autor:
Ledy Ruth Sandoval Fernández

II. ASPECTOS DE VALIDACION

0-20% = Deficiente 21-50% =Regular 51-70% Bueno 71-80%= Muy Bueno 81-100%=Excelente

PREGUNTAS	Claridad en la redacción	Coherencia interna	Lenguaje adecuado	Nivel de entendimiento	Pertinente para los objetivos	Facilidad de comprensión	Inducción a la respuesta	TOTAL
	CALIFICACION DEL NIVEL DE ACEPTACION DE LAS PREGUNTAS							
P1								74%
P2								72%
P3								75%
P4								78%
P5								80%
P6								75%
P7								77%
P8								80%
P9								83%
P10								76%
P11								74%
P12								78%
P13								80%
TOTAL DE RESULTADOS								
PROMEDIO DE VALIDACIÓN								

I. PROMEDIO DE VALIDACIÓN: 77.07%

II. OPCION DE APLICABILIDAD

(X) El instrumento puede ser aplicado, tal como está elaborado.
( ) El instrumento debe ser mejorado antes de ser aplicado.

En caso el instrumento no deba ser aplicado por favor justifique su opinión

Fecha: 06/03/2019

Firma del experto
Mg. Maruja Blas Rebaza

ANEXO 5: Matriz de consistencia

Matriz de consistencia

Modelo de buenas prácticas aplicando Iso 27002 para gestión de incidencias de la red Wncor.

PROBLEMAS	OBJETIVOS	HIPÓTESIS	OPERACIONALIZACIÓN		METODOLOGIA
			VARIABLES	INDICADOR	
Problema General ¿De qué manera el modelo de buenas prácticas aplicando ISO 27002 mejorará la gestión de incidencias de la red Wncor? **Problema Especifico** ¿De qué manera el modelo de buenas prácticas aplicando ISO 27002 reducirá los problemas de conexión de la red Wncor? ¿De qué manera el modelo de buenas prácticas aplicando ISO 27002 reducirá los problemas de ingreso a los file server?	**Objetivo General** Implementar un modelo de buenas prácticas aplicando ISO 27002 para mejorar la gestión de incidencias de la red Wncor. **Objetivos Específicos** Analizar como el modelo de buenas prácticas aplicando ISO 27002 reduce los problemas de conexión de la red Wncor. Analizar en qué medida el modelo de buenas prácticas aplicando ISO 27002 reduce los problemas de ingreso a los file server de la red Wncor.	**Hipótesis General** La Implementación del modelo de buenas prácticas aplicando ISO 27002 mejorará la gestión de incidencias de la red Wncor. **Hipótesis Especifico** El modelo de buenas prácticas aplicando ISO 27002 reducirá los problemas de conexión de la red Wncor. El modelo de buenas prácticas aplicando ISO 27002 reducirá los problemas de ingreso a los file server de la red Wncor.	**<u>Independiente</u>:** Modelo de buenas prácticas. **<u>Dependiente</u>** Gestión de incidencias de la Red Wncor.	➢ Fallas de conexión a la red Wncor ➢ Fallas de ingreso a File Server	▪ **Tipo de investigación** - Aplicada ▪ **Nivel de investigación** - Correlacional ▪ **Metodología** - Cuantitativa, ISO 27002 ▪ **Población** - Datos de Interacción Año Interbank ▪ **Muestra** -Datos de interacción de meses -Usuarios de Interbank. ▪ **Muestreo**

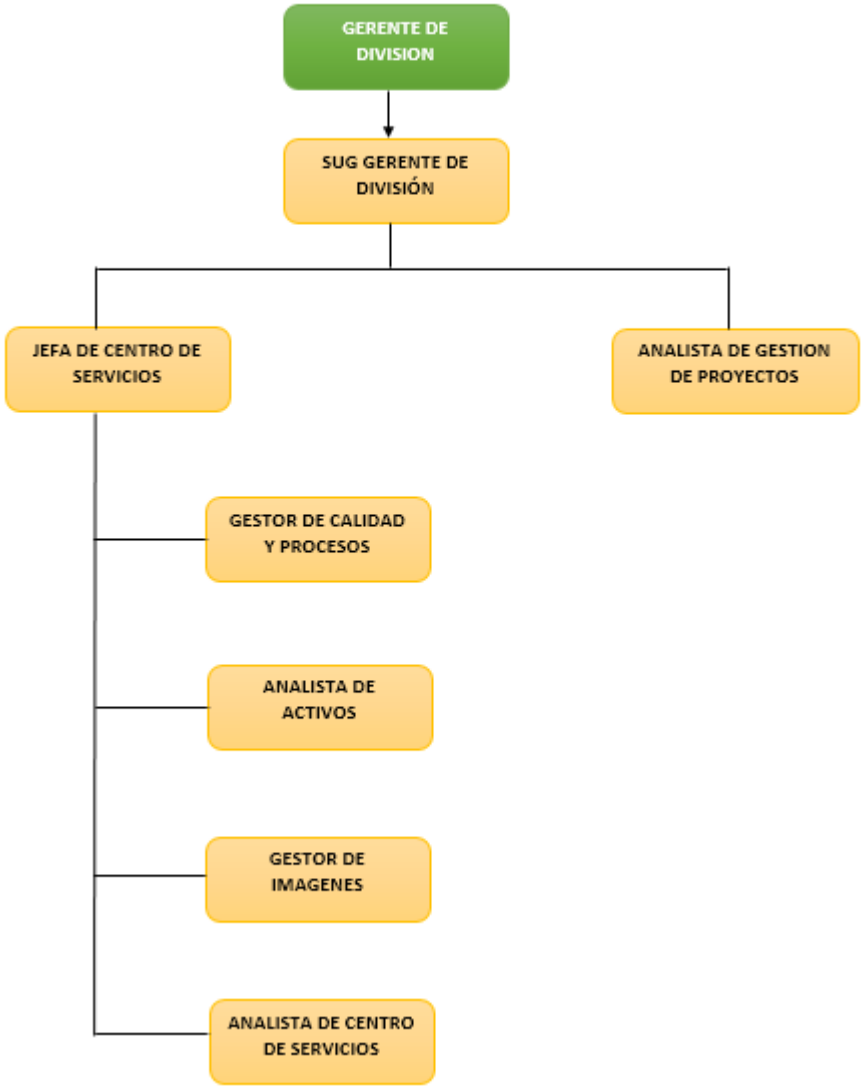
					- Aleatorio simple. ▪ **Procesamiento de Datos** - Software SPSS. ▪ **Técnicas de investigación y aplicación de instrumentos** -Técnica de encuestas y observación Instrumento Ficha de Registro y cuestionario.

ANEXO 6: Organización

Para la realización del presente análisis se requiere establecer el organigrama e identificar las partes involucradas que actuaran en la realización de las actividades y tratamiento de la información.

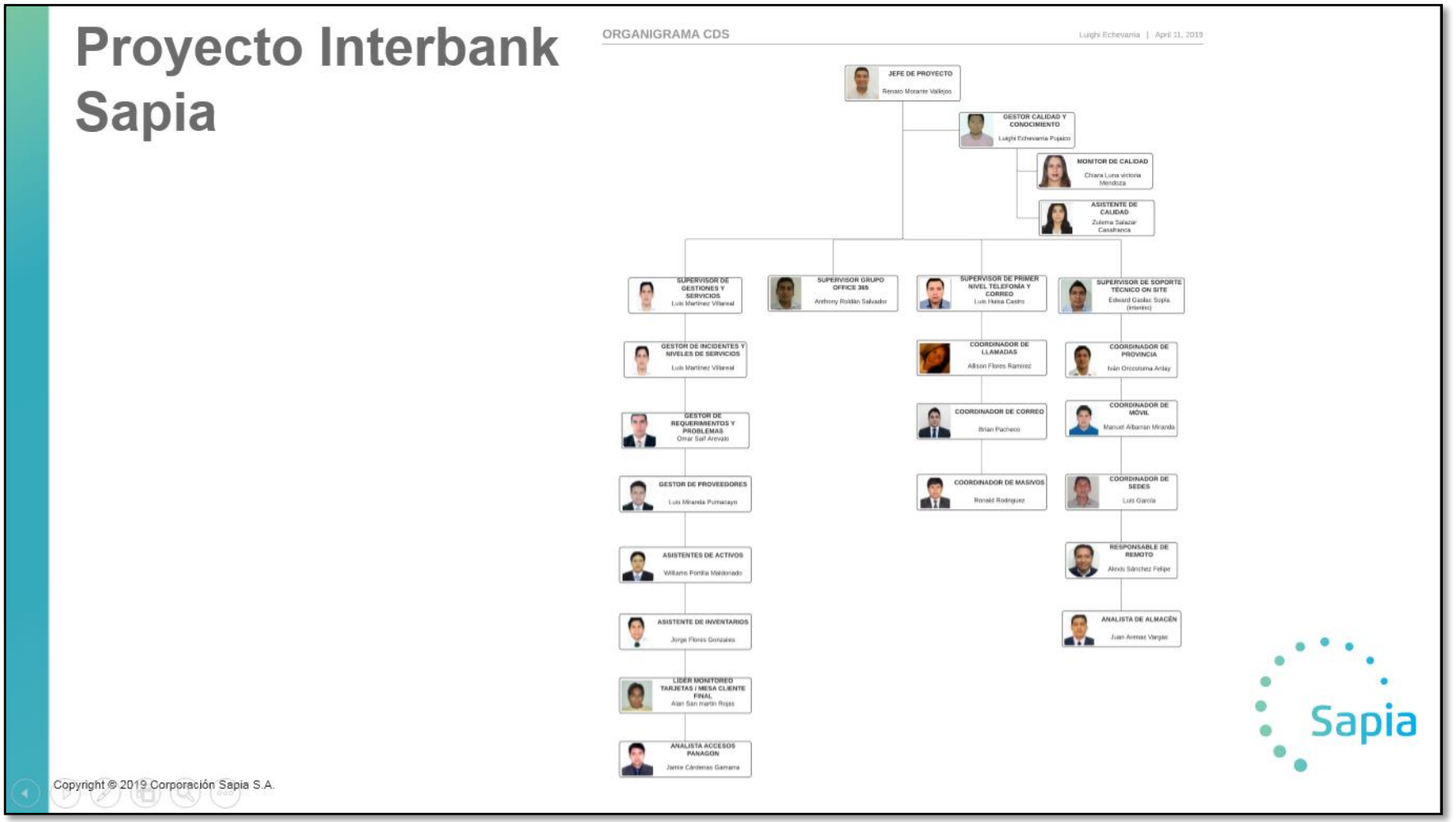
ORGANIGRAMA INTERBANK

A continuación, se muestra el organigrama de los líderes de Interbank que encabezan la supervisión que el Centro de Servicios Brinda a los usuarios.



ORGANIGRAMA SAPIA (CENTRO DE SERVICIOS)

A continuación, se muestra el organigrama de Centro de servicios con todo el personal encargado de brindar el Servicio de calidad a los usuarios de Interbank, encabezando el Jefe de Proyecto junto con supervisores coordinadores y Analistas.



ANEXO 7: Flujograma de la atención que brinda cds a usuarios de Interbank