UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

ESCUELA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

PROYECTO DE INVESTIGACIÓN

TEMA:

"AMENAZAS, VULNERABILIDADES Y SU INCIDENCIA EN EL SISTEMA INFORMÁTICO DE LA RED CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT E.P LOS RÍOS".

Autor:

Sanchez Melendres Karla Yleana

Babahoyo – Los Ríos – Ecuador

2022

DEDICATORIA:

Este proyecto de investigación se lo dedico a Dios, quien supo guiarme por el buen camino y a mis padres por siempre ayudarme a salir adelante.

Y en especial a mi madre, quien es la persona que me enseñó a ser quien soy, a no decaer cuando no tengo fuerzas y ser siempre mi pilar fundamental por quien lucho cada día de mi vida.

AGRADECIMIENTO

En primera instancia agradezco a la Universidad Técnica de Babahoyo por haberme permitido ser parte de ella, así como también a los diferentes docentes que me brindaron sus conocimientos y apoyo para seguir cada día mejorando en mis estudios de mi ardua carrera.

Agradezco también a Dios por darme la sabiduría de haberme permitido llegar hasta aquí, a mi madre y mi pareja por todo su apoyo incondicional, gracias por confiar en mi.

RESUMEN

Se desarrolla la presente investigación titulada: AMENAZAS, VULNERABILIDADES Y SU INCIDENCIA EN EL SISTEMA INFORMÁTICO DE LA RED CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT E.P LOS RÍOS con el fin de estudiar la problemática de la seguridad de la información, que es uno de los aspectos que ha logrado tomar el mayor de los intereses en el campo informático que representa la corporación, para esto, se ejecuta una investigación documental, donde se toman conceptos de autores nacionales e internacionales sobre la Seguridad de la Información , sus riesgos y amenazas. mediante encuestas dirigidas a los directivos, empleados y clientes de la CNT EP Los Ríos, sé evidencia que existen inconvenientes dentro de la empresa y su sistema de seguridad de la información. No se aplica correctamente lo establecido. Así mismo, se ha necesitado fortalecer muchos temas relacionados con la seguridad de la información y las normas ISO 27001, en el estos resultados evidenciados permitieron dar forma a una propuesta que se adapta a la realidad de la corporación, mejorando lo que se ha creído conveniente para la continuidad de la empresa.

Palabras Claves: seguridad de la información, amenazas, riesgos, gestión de talento humano,

ÍNDICE

Índice de cuadros

Índice de gráficos

Índice de figuras

Índice de tablas

1.- Introducción

En los últimos siglos, el desarrollo tecnológico, ha sido el más grande en la historia, y la rápida evolución de la informática en los últimos años, las computadoras el internet y el desarrollo de las Tecnologías de la información han cambiado la forma en que el ser humano percibe el mundo. Es evidente debido a su crecimiento exponencial, que el sistema digital, ha cambiado fuertemente la cultura, y se podría decir que es necesario el utilizar una computadora para casi todo el quehacer humano.

En el siglo XXI, el entorno de los negocios, la mayor ventaja de una computadora con acceso a internet consiste en la enorme cantidad de información lo que es equivalente a poder acceder a la mayor biblioteca disponible al alcance de la mano. Entre otras ventajas las terminales con conexión a red, el acceso a las diferentes variedades de información y la forma en que la misma puede ser manipulada. Conscientes de que la informática presta la utilidad que a todos los ámbitos del quehacer humano y en este contexto, también es muy importante tener presente el cómo guardar la información y protegerla de las posibles amenazas que puedan aparecer.

Los cambios tecnológicos en la actualidad, y debido a que éstos permiten efectuar también operaciones ilícitas, como resultado del gran aumento de la tecnología de la información para mejorar su desempeño, de igual forma se ha desarrollado muy rápido un lado negativo e inseguro que amenaza a todas las redes de información con las que nos vemos envueltos hoy en día, es por ello que las organizaciones se han ido adaptando y acogiendo la **seguridad informática** en sus operaciones, este es el ámbito que trata esta tesis.

Ha crecido marcadamente años recientes, la necesidad de mejorar la seguridad informática de operaciones esto es consecuencia del enorme incremento del uso de la tecnología información como herramienta para mejorar el desempeño, así como las presiones competitivas, producto de la globalización, incremento número de regulaciones, disminución de

instalaciones para reducir costos, con disminución resultante y capacidad de reserva

La seguridad informática consiste en resguardo información que se maneja por medios magnéticos, y en ella está incluida toda clase archivos, sean estos personales, corporativos, financieros, ambientales, estadísticos, institucionales, etc. En este sentido varias organizaciones están dedicando sus esfuerzos desarrollar planes de acción dirigidos a resguardar y proteger la información de cualquier tipo de empresa u organización, como es el caso del:

- Instituto de Seguridad de Computadoras (CSI), publico la encuesta Mundial del Crimen y la Seguridad en las Computadoras, con la participación de la escuadra de intrusión en computadoras de la oficina federal de investigaciones (FBI)en San Francisco, ha informado en su encuesta del 2005 que las perdidas que sufrieron 186 de los que respondieron a las encuestas totalizaron aproximadamente 378 millones de dólares. Estas pérdidas se basan en graves violaciones de seguridad de computadoras detectadas principalmente por grandes corporaciones, agencias de gobierno y universidades.

De acuerdo a la encuesta las violaciones de seguridad detectadas por los que respondieron indican diversos tipos de ataques como: acceso no autorizado por parte de personal de la misma entidad, negativa de servicio, penetración de sistemas de elementos ajenos a la entidad, robo de información protegida por derechos de propiedad intelectual, fraude financiero y sabotaje de datos y redes.

Cuando los sistemas de Control Supervisor y Adquisición de Datos (SCADA) usan la Internet para vigilar y controlar procesos en sitios distantes, son particularmente vulnerables. Tal práctica la emplea una variedad de industrias, entre ellas la petroquímica, elaboración de alimentos, pulpa y papel, productos, química, farmacéuticos, telecomunicaciones, ambientales, transporte, etc.

Este proyecto se origina ante un problema concreto que es: LA INSEGURIDAD INFORMÁTICA, la misma que afecta a varios sectores de empresas tanto públicas, como privadas. Esto es la carencia de sistemas de seguridad que permitan mantener a salvo la información es decir tener estrategias adecuadas para la seguridad informática.

Personalmente, esta investigación busca justificar la necesidad de implantar una propuesta de seguridad informática que cuente con los elementos necesarios que disminuyan significativamente la magnitud de este problema en un grado significativo, para lo que se elaboró el siguiente trabajo que está conformado de tres capítulos, más los anexos que respaldan la investigación:

En el primer capítulo se presenta el abordaje de todo lo referente al problema, como lo es su contextualización, planteamiento, delimitación, justificación y objetivos. es decir, es aquí donde se revisan los antecedentes que dieron origen a esta problemática planteada

Posteriormente se revisa el tema desde su marco teórico referencial formulando la postura teórica, así como las hipótesis y sus variables. Es aquí donde abordamos los diferentes tipos de riesgos informáticos, virus y se muestran algunos ejemplos de posibles daños ocasionados a la empresa CNT EP Los Ríos.

Y por ultimo se determina la metodología de la investigación, en donde describe el tipo, técnica y métodos, así como la respectiva muestra en base a la población resultante.

CAPITULO I.- DEL PROBLEMA

1.1- Idea o tema de Investigación.

Amenazas, vulnerabilidades y su incidencia en el sistema informático de la red Corporación Nacional de Telecomunicaciones CNT E.P Los Ríos.

1.2 Marco Contextual.

1.2.1 Contexto Internacional.

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Referente a los delitos informáticos, entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile.

Dado lo anterior a continuación se mencionan algunos aspectos relacionados con la ley en los diferentes países, así como con los delitos informáticos que persigue.

- Estados Unidos.

  Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los

actos de transmisión de virus. Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática. En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

- Alemania.

  Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

  Espionaje de datos.
  Estafa informática.
  Alteración de datos.
  Sabotaje informático.

- Austria.

  La Ley de reforma del Código Penal, sancionada el 22 de diciembre de 1987, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además, contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

- Gran Bretaña.

  Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta

cinco años de prisión o multas. Esta ley tiene un apartado que específica la modificación de datos sin autorización.

- Holanda.

  El 1º de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

  El hacking.

  El preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio).

  La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría).

  La distribución de virus.

- Francia.

  En enero de 1988, este país dictó la Ley relativa al fraude informático, en la que se consideran aspectos como:

  Intromisión fraudulenta que suprima o modifique datos.

  Conducta intencional en la violación de derechos a terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.

  Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión.

  Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

- España.

  En el Nuevo Código Penal de España, se establece que al que causare daños en propiedad ajena, se le aplicará pena de prisión o multa. En lo referente a:

  La realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos

electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa.

En materia de estafas electrónicas, el nuevo Código Penal de España, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

- Chile.

  Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigor el 7 de junio de 1993. Esta ley se refiere a los siguientes delitos:

  La destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

  Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.

  Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

1.2.2 Contexto Nacional.

En el contexto Nacional, Ecuador ocupa el puesto número 14 a escala regional y el 98 a nivel mundial en el último Índice Global de Ciberseguridad (GCI, por sus siglas en inglés). Se trata de un ranking que analiza el compromiso con la ciberseguridad por parte de por 194 Estados miembros de la Unión Internacional de Telecomunicaciones (ITU) y comprende cinco áreas a examinar: legal, técnica, organizacional, creación de capacidad y cooperación. Con el análisis de estas cinco variables se suma y se agrega en una

puntuación global que categoriza a cada país en una lista que va del más seguro a los más inseguros.

En entrevista con EXPRESO, Gabriel Llumiquinga, presidente de la Asociación Ecuatoriana de Ciberseguridad (AECI), confiesa que esos puntajes reflejan cómo el país sigue rezagado en temas de ciberseguridad en comparación de sus países vecinos y desde hace varios años viene arrastrando “números rojos” respecto a esta materia. Eso quedó evidenciado, por ejemplo, en el ‘Data Breach’ (violación de datos) del caso Novaestrat en 2019, que generó un escándalo por la filtración de datos de millones de ecuatorianos.

Fue ahí, según Llumiquinga, cuando se generaron algunas iniciativas respecto a las políticas públicas de ciberseguridad o con temas relacionados la protección de datos personales, sin embargo, el experto señala que aún no se ha concluido con esas "tareas pendientes" puesto que las propuestas siguen en discusión en la Asamblea. El representante de AECI manifiesta que se trata de algo preocupante teniendo en cuenta el incremento de los delincuentes y delitos informáticos a raíz del confinamiento por la pandemia de coronavirus. Y es que, aunque hay aspectos alentadores que reflejan un leve crecimiento en la importancia de la gestión en ciberseguridad que tienen las compañías, todavía existen otras realidades dentro de las organizaciones que las mantienen lejos de tener **prácticas maduras y efectivas de ciber-riesgos**, que sí se están implementando en las grandes compañías a escala mundial.

Así lo deja claro un informe realizado por la firma Deloitte con la participación de la OEA y en el que también colabora AECI. El trabajo, que encuestó a cerca de 100 empresas a escala nacional, reflejó los siguientes datos:

Ecuador ocupa el puesto 14 a nivel regional y el 98 en el último índice global.

La banca y las empresas de seguro son las que mas invierten en ciberseguridad. Desde 25.00 hasta 100.000

Mas del 50% de las empresas cuentan con herramientas básicas de seguridad (firewalls y antivirus) , mientras solo un 3% de las empresas en el país cuentan con soluciones que reducen estos riesgos como Cloud Acces, Security Broker

Solo el 20% de empresas realizan actividades de vigilancia como ciberamenazas.

Para Llumiquinga, este fenómeno se da en parte porque no existe la “plena conciencia” de la importancia de la ciberseguridad en el país, además de la carencia de una política pública transversal para todos los sectores en esta materia.

1.2.3 Contexto Local

Los Ríos, Provincia de la costa ecuatoriana, se encuentra ubicada en la cuenca hidrográfica del río Guayas, en el centro – sur – oeste de la República del Ecuador. Es la única provincia de la región que no tiene acceso al mar. Cuenta con una extensión de 7.177,62 Km2, y, tiene una población de 778115 habitantes, de los cuales según el género corresponden a 398099 hombres y 380016 mujeres. Políticamente se encuentra dividida en trece cantones, siendo su capital, la ciudad de Babahoyo, el cantón Babahoyo posee un total de 153776 habitantes, según el género corresponden a 77967 hombres y 75809 mujeres. (inec.gob.ec, 2010).

.

El cantón Babahoyo, está dividido en cuatro parroquias rurales y cuatro parroquias urbanas, estas últimas se asientan en la ciudad de Babahoyo, siendo las parroquias El Salto, Barreiro, Clemente Baquerizo y Camilo Ponce Enríquez. La ciudad de Babahoyo tiene aproximadamente en su entorno urbano 82500 habitantes.

El desarrollo de la economía provincial se debe a su estratégica ubicación geográfica en el país, ya que su localización está en el centro de la cuenca del río Guayas, es una zona altamente rica y con las mejores proyecciones económicas del Ecuador.

Los Ríos es parte importante del conjunto de las siete provincias del litoral ecuatoriano que genera el 42,30% de las divisas no petroleras (alrededor de 75 818 millones de dólares cada año). La Provincia genera más de 2000 millones de dólares como producción bruta al año, aproximadamente el 2,63% del total nacional.

La Población Económicamente Activa (PEA) de Los Ríos, está conformada por 292 772 personas, de las cuales 25,87% son mujeres. En base al PEA, el cantón Quevedo representa el 23,39%, Babahoyo el 20,53%, Ventanas el 8,48% y Vinces el 8,82%; en estos sectores se realiza la mayor actividad comercial, bancaria y de servicios.

De la población económicamente activa, el 42,17% de las personas se dedica al sector primario, el 36,37% está en el sector terciario y el 8,63% a las actividades del sector secundario.

No obstante, pese a la información recopilada no se cuenta con datos concretos sobre los ataques de ciberseguridad específicos en la provincia de los Ríos

1.2.4 Contexto Institucional.

Con la resolución 4458 suscrita el 24 de octubre de 2008, el superintendente de Compañías, Pedro Solines, aprobó la fusión entre Andinatel S.A. y Pacifictel S.A., y la creación de la Corporación Nacional de Telecomunicaciones CNT S.A, que absorbe a ambas telefónicas, tendrá su sede en Quito por una duración de 50 años y arrancará con un capital de $ 245’920.000 dividido en 2’459.000 acciones ordinarias de $ 100 cada una. El 14 de enero de 2010 mediante decreto ejecutivo No. 218, publicado en Registro Oficial 122 en el gobierno de Rafael Correa, la Corporación Nacional de Telecomunicaciones CNT S. A. pasa a ser entidad pública denominándose CNT EP (Corporación Nacional de Telecomunicaciones Empresa Pública). Alegro PCS (Telecsa) fue una compañía del Ecuador con sede en Quito que operaba servicios de telefonía móvil e internet, creada por Andinatel y Pacifictel para ofertar el servicio de telefonía móvil en el territorio ecuatoriano.

El 3 de abril de 2003 recibió la concesión de parte del Estado ecuatoriano, entrando a iniciar sus operaciones bajo la marca Alegro PCS en diciembre de ese año.

En marzo de 2010 es anunciado que la Corporación Nacional de Telecomunicaciones, CNT EP absorberá a la compañía Alegro PCS para salvar

a la empresa de la quiebra por las pérdidas acumuladas, pasando a ser propiedad del estado ecuatoriano.

Posteriormente, el 3 de agosto de 2010 César Regalado, gerente general de la CNT-EP y Jaime Guerrero, ministro de Telecomunicaciones y de la Sociedad de la Información, firmaron el convenio con el cual CNT-EP absorbe los pasivos de la empresa de telefonía móvil, oficializándose la fusión de la Corporación Nacional de Telecomunicaciones, CNT-EP con la empresa de telefonía móvil Alegro.
En octubre del 2010 CNT EP suscribió con el Superintendente de Telecomunicaciones subrogante, Claudio Rosas, la concesión de la banda 11.45–12.2 GHz (downlink), para la operación del sistema de audio y video por suscripción, bajo la modalidad de televisión codificada por satélite. La compañía Media Networks, con sede en Perú, ganó la licitación para implementar el sistema Direct-to-Home (DTH) que consiste en una antena que recibe la señal satelital, que es instalada en las terrazas de las viviendas.

César Regalado, gerente de la CNT EP, el 22 de noviembre de 2011 realizó el lanzamiento del servicio de televisión satelital pagada de la empresa pública el cual toma como acrónimo CNT TV.

CNT TV entró al mercado de televisión por suscripción ofertando un paquete básico8 junto a paquetes complementarios más un costo adicional, logrando competir con los servicios que operan en el país, como TV Cable, Claro TV, DirecTV, entre otras.

A mediados de diciembre del 2013, la Corporación Nacional de Telecomunicaciones (CNT-EP) empezó a comercializar el paquete premium HBO/MAX para su servicio de DTH, incorporando al plan básico nueve canales SD y cinco HD de HBO Latin America Group, sin costo adicional.

La Corporación Nacional de Telecomunicaciones CNT EP, mediante estaciones base 4G LTE base stations y el sistema de gestión 5620 SAM de Alcatel-Lucent, despliega la primera red de banda ancha móvil 4G LTE en el

territorio ecuatoriano, que cubrirá inicialmente a Quito, Guayaquil, Ambato, Manta, Portoviejo y Santo Domingo, posteriormente extenderá la señal LTE a las principales ciudades del país1 y a las zonas rurales del Ecuador, donde la cobertura actual es limitada o inexistente.

Con la implementación de la tecnología, la CNT EP planea mejorar la capacidad de su red de datos y ampliar la cobertura nacional, incluyendo el despliegue de nuevos servicios como el video de alta definición, telepresencia, e-learning y seguridad pública.

El servicio comenzó a ofrecerse al público en general desde diciembre del 2013, cubriendo inicialmente las ciudades de Quito y Guayaquil.
A inicios del año 2015, el gerente de publicidad y marca de la Corporación Nacional de Telecomunicaciones (CNT), Alexander Gómez, sostuvo que CNT Play busca acortar la brecha entre los productores independientes y los canales de difusión, siendo este servicio una ventana para ofrecer sus contenidos. Este servicio es básicamente una plataforma de video streaming de contenidos con un enfoque en la producción nacional.

El 1 de junio 2019 la Corporación Nacional de Telecomunicaciones efectúa un cambio a su estructura organizacional eliminando las Gerencias de Agencia Provincial y dejando solo Gerencias Nacionales y Regionales, situación que concentra demasiado las operaciones y vuelve lento el desarrollo de las agencias provinciales.

1.3. Situación problemática.

En el mes de julio 2021, CNT (Corporación Nacional de Telecomunicaciones) fue víctima de un ataque informático. Esto pone en el objetivo las políticas de ciberseguridad con el que deben contar todas las empresas e instituciones y que da de qué hablar en el Ecuador.

La Corporación Nacional de Telecomunicaciones (CNT) durante julio del 2021 ha denunciado dos ataques informáticos a sus bases de datos. Las autoridades denunciaron ante la Fiscalía los hechos.

1.4-Planteamiento del problema.

CNT indicó que el 22 de julio la entidad sufrió un ataque informático que interrumpió los canales de atención a los clientes. Además, dijo que el ataque no ha puesto en riesgo la información privada de los clientes, ni el funcionamiento de los servicios.

Asimismo, el pasado 16 de julio CNT señaló que fue víctima de un ataque informático el miércoles 14. A través de un comunicado informó que presentó una denuncia en la Fiscalía para que la entidad dé con los autores del delito.

Fuente diario el comercio 28 de julio de 2021 21:18

1.4.1.- Problema.

¿Cómo implementar un adecuado sistema de detección de las amenazas y debilidades del sistema informático de la Corporación Nacional de Telecomunicaciones?

1.4.2.- Subproblemas o derivados.

- ¿Cuenta actualmente con un sistema de detección de amenazas la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos?
- ¿Por qué el sistema actual de detección de amenazas no cumple con las expectativas que los usuarios requieren afectando la calidad en la atención en la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos?
- ¿Cómo el sistema de detección de amenazas y debilidades de los sistemas informáticos afectan la calidad en la atención y no contribuyen al desarrollo y crecimiento de la organización en la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos?

1.5. Delimitación de la investigación

1.5.1- Objeto de estudio:

El sistema de políticas de seguridad de la información de CNT EP Los Ríos**.**

1.5.2.- Campo de acción:

La gestión de la calidad de atención a los clientes internos.

1.5.3- Temporal

De marzo a abril 2022

1.5.4- Espacial

Organización: Corporación Nacional de Telecomunicaciones CNT EP Los Ríos**.**

Ubicación:

- Parroquia Camilo Ponce Enríquez.
- Ciudad Babahoyo.
- Cantón Babahoyo.
- Provincia de Los Ríos

1.5.5- Unidades de observación

- Directivos: 3(Tres)
- Administrativos: 6 (Seis)
- Personal de Servicios: 2 (Dos)
- Personal técnico de operaciones: 12 (Doce)
- Técnicos Integrales: 50(cincuenta)
- Personal comercial: 30 (treinta)
- Clientes: 20000 (veinte mil)

1.6.- Justificación.

La seguridad informática es una necesidad presente en cualquier institución, cuando se tienen protocolos, controles y procedimientos que permitan verificar que los objetivos de continuidad de servicio, confidencialidad y seguridad de la información, se cumpliría satisfactoriamente con las características primordiales de la información, y así se prevería la alteración de sistemas, ataques y accesos no autorizados. Es por esto que una propuesta de seguridad en la información son las bases para que cada usuario tenga una protección en sus estaciones de punto final en la red de la empresa. Si las organizaciones tuvieran protección en su información y la seguridad adecuada, existiría la defensa idónea para sus activos de información.

1.7-Objetivos

1.7.1- Objetivo.

Potenciar el sistema de seguridad informática en la Corporación Nacional de Telecomunicaciones CNT EP Agencia Los Ríos para lograr mejorar la productividad de la empresa.

1.7.2- Objetivos específicos.

- Fundamentar de Bases Teóricas confiables, los sistema de detección de amenazas y la seguridad informática.
- Identificar las necesidades y exigencias actuales de la CNT EP para diseñar adecuadamente estrategias de seguridad informática.
- Proponer estrategias adecuadas que permitan potenciar los sistemas de seguridad informática de CNT EP.

CAPÍTULO II.- MARCO TEORICO O REFERENCIAL

2.1. Marco teórico.

La seguridad informática se presenta como una necesidad que se fundamenta en el establecimiento de controles e implantación de procedimientos y métodos con el objetivo administrar y proteger el activo de la información

2.1.1. Marco conceptual.

2.1.1.1- AMENAZAS

DEFINICIÓN

Microsoft (2016):

> *La Amenaza es la probabilidad de ocurrencia de un suceso potencialmente desastroso durante cierto periodo de tiempo, en un sitio dado. En general el concepto de amenaza se refiere a un peligro latente o factor de riesgo externo, de un sistema o de un sujeto expuesto, expresada matemáticamente como la probabilidad de exceder un nivel de ocurrencia de un suceso con una cierta intensidad, en un sitio específico y durante un tiempo de exposición determinado. (Consultado 15.04.2016).*

Una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño en los sistemas de información, produciendo pérdidas materiales, financieras o de otro tipo. Las amenazas son múltiples desde una inundación, un fallo eléctrico o una organización

criminal o terrorista. Así, una amenaza es todo aquello que intenta o pretende destruir.

TIPOS DE AMENAZAS

Amenazas Humanas

Surge por ignorancia en el manejo de la información, por descuido, por negligencia, por inconformidad. Para este caso se pueden considerar a los hackers, crakers, phreakers, carding, trashing, gurús, lamers o scriptkiddies, copyhackers, bucaneros, newbie, wannabers, samurai, creadores de virus y los que se listan a continuación:

Figura 1. Amenazas Humanas.

Ingeniería social: es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan de forma que revelen datos indispensables que permitan superar las barreras de seguridad. Esta técnica es una de las más usadas y efectivas al momento de averiguar nombres de usuarios y contraseñas.

Ingeniería social inversa: consiste en la generación, por parte de los intrusos, de una situación inversa a la original en la ingeniería social. En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios y éstos lo llaman ante algún imprevisto. El intruso aprovechará esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el propio.

Robo: Las computadoras son las posesiones más valiosas de la empresa y se encuentran expuestas. Es frecuente que los operadores utilicen las computadoras de las empresas para realizar trabajos privados o para otras organizaciones y de esta manera robar tiempo de máquina.

Fraude: Cada año millones de dólares son sustraídos de las empresas y, en muchas ocasiones, las computadoras son utilizadas para dichos fines. Es uno de los problemas más habituales de las Organizaciones, sea del tipo que sea y a todos los niveles, ya que se refiere al perjuicio económico patrimonial realizado con ánimo de lucro y llevado a cabo con engaño. El fraude no trata más que lograr un beneficio ilegal reduciendo las propiedades de la compañía.

Sabotaje: El sabotaje ha sido utilizado desde la antigüedad, partiendo del axioma de "una eficiencia máxima, con unos medios y un riesgo mínimo para el saboteador. Para lograr estos fines el saboteador tratará de determinar los puntos débiles de la organización y estudiará las posibilidades de acceder a las áreas donde mayor daño pueda hacer. Es el peligro más temido en los centros de procesamiento de datos, ya que éste puede realizarlo un empleado o un sujeto ajeno a la empresa.
Personal: De los robos, fraudes, sabotajes o accidentes relacionados con los sistemas, el 73% es causado por el personal de la organización propietaria de dichos sistemas.

Personal interno: Son las amenazas al sistema provenientes del personal del propio sistema informático. Los daños causados por el personal pueden ser accidentales, deliberados o productos de la negligencia. Los recursos y programas, así como la información, deben estar especialmente protegidos contra estos tipos de daños.

Ex-empleado: Generalmente son personas descontentas con la organización y que conocen a la perfección la estructura del sistema, por consiguiente, tienen los conocimientos necesarios para causar cualquier tipo de daño.

Curiosos: Son personas que tienen un alta interés en las nuevas tecnologías, pero aún no tienen la experiencia ni conocimientos básicos para considerarlos hacker o crackers, generalmente no se trata de ataques dañinos, pero afecta el entorno de fiabilidad y confiabilidad generado en un sistema.

Terrorista*:* En esta definición se engloba a cualquier persona que ataca al sistema causando un daño de cualquier índole en él, tienen fines proselitistas o religiosos.

Intrusos remunerados: Se trata de crackers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar secretos o simplemente para dañar de alguna manera la imagen de la entidad atacada.

Amenazas de Hardware

Este tipo de amenazas se da por fallas físicas que se encuentra presente en cualquier elemento de dispositivos que conforman la computadora. Los problemas más

identificados para que el suministro de energía falle son el bajo voltaje, ruido electromagnético, distorsión, interferencias, alto voltaje, variación de frecuencia, etc.

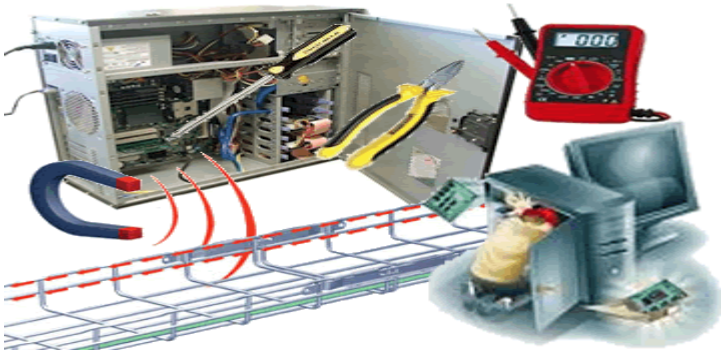


Figura 2. Amenazas de Hardware.

Amenazas de Red

Se presenta una amenaza cuando no se calcula bien el flujo de información que va a circular por el canal de comunicación, es decir, que un atacante podría saturar el canal de comunicación provocando la no disponibilidad de la red. Otro factor es la desconexión del canal.

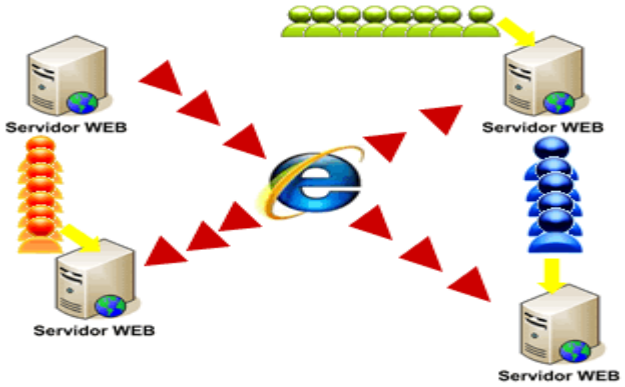


Figura 3. Amenazas de Red.

Amenazas Lógicas

La amenaza se hace presente cuando un diseño bien elaborado de un mecanismo de seguridad se implementa mal, es decir, no cumple con las especificaciones del diseño. La comunicación entre procesos puede resultar una amenaza cuando un intruso utilice una aplicación que permita evitar y recibir información, ésta podría consistir en enviar contraseñas y recibir el mensaje de contraseña válida; dándole al intruso elementos para un posible ataque.

En la mayoría de los sistemas, los usuarios no pueden determinar si el hardware o el software con que funcionan son los que supone que deben ser. Esto facilita al intruso para que pueda reemplazar un programa sin conocimiento del usuario y éste pueda inadvertidamente teclear su contraseña en un programa de entrada falso al cual también se le denomina códigos maliciosos.

Los tipos de códigos maliciosos más comunes son: caballos de Troya, virus, gusanos, bombas de tiempo y keyloggers.

FRAUDE

Se entiende por fraude los delitos ¨ cometidos por manipulación de computadoras en los que se distinguen: la manipulación de datos de entrada, abarcando a la sustracción o apoderamiento de estos, y la manipulación de programas. ¨

FALSIFICACION

Otro delito importante de tomarse en cuenta es la falsificación, que últimamente ha aumentado considerablemente. Debido al panorama de amenazas cambiantes, este ha cobrado relevancia en todo el mundo, el documento de la ONU lo describe como conductas de : ¨adulteración de la información contenida en forma de datos , o como la alteración de documentos almacenados en los sistemas¨.

DAÑAR O ALTERAR PROGRAMAS DE DATOS

En la actualidad existen riesgos significativos que se deben prevenir de una manera eficaz, como es: el daño o alteración de sistemas y lo clasifican en distintas acciones como: ¨sabotaje informático, envío de virus , gusanos, bombas lógicas, accesos no autorizados, reproducción no autorizada de programas ¨

2.1.1.2.- SISTEMA DE INFORMACION

DEFINICIÓN

Antes de involucrarnos de lleno al tema citado anteriormente, es importante conocer algunos conceptos importantes para la óptima comprensión del tema.

Datos: hechos coleccionados, sin procesar y que son identificados simbólicamente con letras, números, valores, resultados, etc.

Información: hechos procesados dotados de relevancia y con algún propósito, dentro del entorno en el que se desarrollan y que presentan algún valor.

Sistema: módulo de elementos que se encuentran interrelacionados, ordenados y que interactúan entre sí.

Sistema de Información: encargado de brindar información con algunos atributos importantes que ayudan a realizar alguna operación, tomar una decisión, en el momento que se necesita.

Atributos de la información

- Comprensión: Debe ser entendible.
- Economicidad: Mínimo costo para obtener esta información.

TIPOS DE SISTEMAS DE INFORMACION

Soporte a las actividades operativas:

- Para actividades estructuradas (aplicaciones de gestión empresarial).

- Actividades menos estructuradas (programas técnicos para funciones de ingeniería, aplicaciones ofimáticas, etc.)

Soporte a las decisiones y el control de gestión:

Que se pueden dar desde las aplicaciones de gestión empresarial o a través de aplicaciones específicas.

Área donde se aplican estos sistemas:

Áreas de la empresa: recursos humanos, marketing, etc.

Enterprise Resource Planning (ERP)

Sistemas de gestión integrados que controlan los procesos de toda la empresa (RH, finanzas, producción, etc.)

Customer Relationship Management (CRM)

Gestión de la relación con clientes y contactos comerciales.

Business Intelligent (BI)

Explotación de datos e información para la toma de decisiones.

Transaction Processing Systems (TPS)

Procesos de transacciones y operaciones.

Management Information Systems (MIS)

Diferencia entre los sistemas de información.

Business Process Management (BPM)

Diseño, ejecución y control de procesos.

Datawarehousing

Almacenamiento de datos procedentes de varias fuentes.

Datamining

Detección y muestra de relaciones entre los datos y obtener cierto tipo de información.

Queries And Reporting

Consultas e Informes de las Bases de Datos relacionales.

Balanced Scorecard

Cuadro de Mando Integral: planificación y control que permite generar estrategias y comprobar su ejecución.

Website Corporativo

Proyección de imagen corporativa, comunicación, coordinación y operaciones empresariales.

Gestión Documental

Soporte a todas las fases de todos los sistemas de gestión documental.

Supply Chain Management (SCM)

Automatización de la cadena de suministros de la organización.

Computer Telephony Integration (CTI)

Integración entre los sistemas informáticos y los sistemas de comunicación telefónica.

Geographical Information System (GIS)

Sistemas de Información Informática, sistema a la gestión de información geográfica (graficas de mapas).

Sistema de Gestión de Seguridad de la Información (SGSI) gestión de seguridad de la información.

Electronic Data Interchange (EDI) Intercambio de información a nivel logístico y comercial.

Computer Aided Desing CAD:

Diseño Asistido por Ordenador, permite realizar planos.

Sistemas De Soporte De Decisiones (DSS)

Es una herramienta de Business Intelligence enfocada al análisis de los datos de una organización, permiten resolver gran parte de las limitaciones de los programas de gestión

2.1.1.3- RIESGOS

DEFINICIONES

TIPOS DE RIESGOS

2.1.1.4.- CODIGO DAÑINO

El código dañino o malicioso ha sido una amenaza para la seguridad de las computadoras de punto final desde hace ya un buen tiempo, debido al impacto negativo que ha tenido para los usuarios de computadoras de punto final, representando también pérdidas para las empresas que dependen de la computadora de punto final como herramienta de trabajo. De acuerdo con Symantec. "el código malicioso se puede obtener de cualquier software que sea descargado de Internet, ya que éste puede contener virus o algún otro tipo de código malicioso. Un mensaje de correo electrónico puede tener un archivo adjunto que contenga un virus. No se pueden ver a simple vista, hasta cuando sea demasiado tarde y pueden incapacitar a la computadora y causar estragos a en archivos.

VIRUS

La definición formal de un virus dice que es un "microbio invisible con el microscopio común, responsable de las enfermedades contagiosas. Los virus

no son capaces de multiplicarse por sí mismos, por lo que precisan invadir otras células vivas

Este concepto es propio de la medicina, pero ha sido tomado por la informática, para llamarle virus informático al programa que contiene código dañino capaz de multiplicarse por sí mismo con este tipo de código y copiarse a sí mismo en otros programas, modificándolos. Con esto se puede deducir que un virus informático es un programa con un comportamiento determinado y tiene un conjunto de instrucciones a realizar. Su objetivo primordial es auto reproducirse"

En términos generales, los virus son programas que infectan documentos o sistemas, mediante la inserción o la agregación de una copia de sí mismo o mediante la reescritura de archivos completos. Los virus trabajan sin el conocimiento ni la autorización del usuario. Por lo tanto, cuando se abre un archivo infectado, el virus incrustado se ejecuta también con frecuencia en segundo plano. Los virus auténticos son propagados por los propios usuarios en casi todos los casos de forma no intencional.

FUNCIONAMIENTO DE LOS VIRUS INFORMATICOS

Un virus es desarrollado por un programador que sabe mucho en esta materia, conocidos en el mundo de la informática underground como "viriis". El virus llega, de alguna manera a las computadoras de punto final, pero éste no puede hacer nada, si no es ejecutado por el usuario, o por algo que active.

El momento de la infección ocurre cuando este programa es ejecutado de alguna manera, entonces "surte efecto el código que contiene, y el virus entra en otro estado, digámosle estado activo, donde busca reproducirse e introducirse al entorno limpio copiándose a sí mismo en otros archivos a los que llamaremos infectados, y con esto se crea un, digámosle, entorno contaminado en el sistema. A partir de este momento el archivo infectado

incluirá un comportamiento tipo virus. Entonces el virus buscará cómo propagarse, a este evento se le llama replicación, y según su naturaleza será la forma de poderse propagar en "entornos limpios, según el tipo de virus del que se trate 35

El virus puede estar presente en un sistema, pero éste no podrá hacer nada si no es ejecutado por algo que lo active, por lo tanto, se puede mantener un "entorno limpio", aunque se tenga algún virus almacenado en disco, a esto se le podría llamar como tener virus en estado latente. A menudo no aparece nada que avise que se va a producir dicha infección antes, de que ya sea un hecho consumado, para entonces, ya puede ser muy tarde para salvar los datos que ya han sido dañados.

La materia de los virus informáticos ha evolucionado con el tiempo, gracias a las facilidades que puede proporcionar un sistema operativo y los medios tecnológicos. Debido a esto, actualmente existen varios tipos de virus, y dependiendo del comportamiento y la técnica de reproducción que utilizan

TIPOS DE VIRUS

Antes de entrar en la clasificación de los virus, es necesario hacer unas aclaraciones acerca de los mismos: el concepto de un virus ya ha sido descrito anteriormente, pero se ha creado gran confusión por las compañías que desarrollan programas antivirus y con apoyo de los medios de comunicación.

Este es el caso de los troyanos, tema que es tratado con más detalle en la sección de troyanos, pues este tipo de programas no son virus: "su comportamiento es muy diferente al de un virus, porque no buscan reproducirse a sí mismos, ni propagarse. Su objetivo principal es obtener acceso remoto con privilegios de administración a un sistema"

La confusión se origina, cuando los programas antivirus los incorporan a este tipo de programas en sus planes para la protección de computadoras de punto final, y les dan la clasificación de virus tipo troyano, pues el objetivo de los

antivirus es garantizar la protección de una computadora de punto final ante código que tiene propósitos maliciosos, y los medios de comunicación han desarrollado la idea de que "los virus informáticos son malos y pueden destruir las computadoras".

Lo mismo sucede con otro tipo de aplicaciones de código malicioso, como los password stealers, nukers, keyloggers, exploits, entre otros, éstas son herramientas de ataque de los intrusos para un propósito específico. Por sus propósitos maliciosos, son tomados en cuenta para la protección de computadoras de punto final en los antivirus.

Aclarando estos conceptos, sólo se mencionan algunos tipos de virus., los más relevantes y comunes son:

tabla 1 Tipos de Virus y sus características

Tipo de Virus	Característica
Virus MBR (Master Boot Record)	Todo disco tiene un sector MBR al principio del disco, donde se guarda información del disco y del tamaño de las particiones, el código de arranque. A pesar de que sea formateado el disco, esta información no se puede destruir, y si esto llegase a ocurrir, entonces el disco queda inservible. Este sector es muy pequeño, tan sólo ocupa 512 bytes, y parte de él la reserva para la tablas de particiones. Los MBR pueden permanecer ahí compartiendo créditos con el código de arranque. Estos tipos de virus son de los más comunes, aunque existen más tipos que no serán tratados, agregándole a esto, que muy a menudo aparecen nuevos virus, y algunos otros tipos derivados de la combinación de los tipos de virus existentes.
Virus compañero	Aquí el virus no se incrusta en el archivo ejecutable (.exe), sino que crea otro archivo con el código del virus y extensión .com. Como MS-DOS carga primero los de extensión .com y luego los .exe, el virus es cargado antes que el programa. Este es un mecanismo muy antiguo.
Virus ocultos en archivos	Estos virus se incrustan en el archivo ejecutable de un programa, y para disimular el incremento del tamaño del archivo, truncan la información del sistema operativo aparentando el mismo tamaño que la versión del archivo sin contaminar. Esto representa un problema, ya que si se pasan utilidades de verificación del disco, cuando comparan el tamaño real con el informado por el sistema operativo, éstos tratan de repararlo y lo dejan inutilizable, aunque posteriormente se le pase un antivirus.
Virus completamente ocultos	Estos tipos de virus no modifican los datos del disco para ocultar su tamaño, sino que permanecen atentos a las llamadas de información del disco para obtener el tamaño de los archivos, y restan el tamaño del virus, para aparentar el tamaño real del archivo sin infectar.
Virus sencillo	Un virus sencillo se activa cuando un usuario arranca un programa infectado. A continuación, el virus toma el control de la computadora y se agrega a otro archivo de programa. Estos virus son fáciles de detectar, dado que crean una copia exacta de sí mismos. Para encontrar estos tipos de virus, los productos de software antivirus sólo tienen que buscar la secuencia de bytes que los caracteriza, conocida como firma.

Virus encriptado	En el caso de los virus encriptados, la firma está encriptada, de modo que el escáner no puede detectarla. La firma del virus cambia de un programa a otro. Sin embargo, la rutina de desencriptación no cambia, de modo que el software antivirus puede buscar una rutina de desencriptación repetitiva, en lugar de buscar la firma. Además de los virus sencillos y encriptados, existen cuatro tipos principales de código malicioso: virus polimórficos, virus de macro, gusanos y caballos de Troya.
Virus polimórfico	Los virus polimórficos de computadora se diseñan para hacer difícil su detección, si bien los programas antivirus pueden detectar y eliminar fácilmente este tipo de virus. Los autores de los virus polimórficos encriptan el cuerpo del virus y la rutina de desencriptación. No existen dos infecciones iguales, de modo que no puede crearse una sola definición antivirus para eliminar todos los virus. Los fabricantes de soluciones antivirus usan su tecnología de protección antivirus para crear rutinas genéricas de desencriptación que dejan al descubierto el virus.
Virus de macro	Los virus de macro, son los más comunes y que con más facilidad se crean. También suelen ser los menos dañinos. Los virus de macro utilizan un lenguaje de macro de aplicaciones (como Visual Basic o VBScript) para infectar y replicar documentos y plantillas. Son independientes de la plataforma, pero suelen estar asociados a los programas que componen Microsoft Office. Estos virus utilizan el entorno de programación de Microsoft para ejecutar automáticamente el código de macro del virus. Cuando se abre el documento infectado, el virus se ejecuta e infectará las plantillas de aplicación del usuario.
Gusanos	Un gusano es un programa que se propaga a sí mismo por una red, normalmente a través de correo electrónico, TCP/IP o una unidad de disco. Se reproduce a sí mismo a medida que se ejecuta. Los gusanos no son técnicamente un "virus", porque pueden propagarse de forma independiente. Muchos programas maliciosos son clasificados como virus cuando en realidad son gusanos. Por ejemplo, I LOVE YOU era un gusano, no un virus. Los gusanos son muy peligrosos para la red y son más difíciles de controlar porque no requieren la ayuda del usuario para propagarse. Pueden propagarse a cientos de miles de computadoras en muy poco tiempo. Imagine una red corporativa en la que varios usuarios reciban y activen el gusano. Resulta sencillo imaginar
	cómo la red se detendría del todo en pocas horas, a causa de la gran cantidad de tráfico generado por el gusano, por no hablar de la pérdida de la información que contuvieran los archivos dañados. Por otro lado, dado que el gusano se propagaba principalmente por correo electrónico, podría infectar con facilidad otras redes, dentro de un periodo de tiempo muy breve.
Virus de Web	Los applets de JAVA y los controles Active X, son unos lenguajes nuevos orientados a Internet, pero las nuevas tecnologías abren un mundo nuevo a explotar por los creadores de virus. De momento no son muy utilizados pero a partir del 2000, superaran en número a los virus de macro.

Tabla 1. Tipos de virus.

IMPACTO DE LOS VIRUS

Uno de los primeros en circular públicamente se convirtió en un virus destructivo. Se llamaba Merrit y apareció en 1987. Este virus podía destruir la tabla de asignación de archivos (FAT) de los disquetes Con el tiempo, Merrit paso por vanas etapas de evolución, de las cuales la más peligrosa se llamo Golden Gate, donde realmente formateaba al disco duro de la victima

En el caso de I LOVE YOU, el gusano solía llegar a los usuarios por correo electrónico, en forma de un archivo adjunto de correo electrónico que contenía un programa basado en VBScript el usuario ejecutaba el archivo adjunto se iniciaban automáticamente varios procesos secundarios que realizaban la copia (la propagación del gusano y lo enviaban en un archivo adjunto de correo electrónico a todas las personas que aparecieran en la libreta de direcciones de Microsoft Outook "El gusano también borraba y sustituía algunos tipos de archivos del disco duro del usuario, de modo que si se abría cualquiera de estos archivos, se ejecutaba de nuevo la rutina de propagación.

Una tendencia actual de los virus, que han evolucionado cada vez más, es atacar servidores y de esa manera propagare Tales son los casos de los casos relevantes del 2003 de los virus tipo gusano "código rojo (red code), y Nimda (admin alreves) Estos virus atacan al servidor Web IIS de Microsoft a través de una vulnerabilidad transversal quienes, si llegan a penetrar en el servidor, to infectan metiendo además trafico a la red, meten puertas traseras a la red, meten puertas traseras y degradan el funcionamiento del equipo.

Datos reportados por el "CERT indican que el gusano "código rojo (Code Red)

infecto más de 250 000 sistemas en tan solo 9 horas.

En caso de Nimda modifica los archivos Web del servidor para introducir códigos maliciosos que afectan algunos navegadores de internet Explorer y clientes de correos Outlook, además de compartir carpetas obteniendo as varios métodos para propagarse por correo electrónico por páginas de internet

hospedadas en servidores Web llS infectados y por carpetas compartides en redes Microsoft.

La mayor parte de las perdidas contabilizadas por las empresas afectadas por virus informáticos se deben a la acción de tres virus de todos conocidos. Code Red se encuentra en primer lugar de este peculiar ranking con unas perdidas estimadas de 32412, millones de dolores seguido a distancia por otro conocido gusano, el Sircam con perdidas ocasionadas por valor de 14045 millones de dólares, el ultimo lugar de la clasificación lo ocupa Nimda con 7724011 millones de dólares.

TROYANOS

Los troyanos son programas maliciosos que están camuflados como programas benignos, por ejemplo protectores de pantalla, aplicaciones de archivos, juegos incluso programas para detectar y destruir virus reales de archivo, juegos o Sin embargo, el programa tiene en realidad una función maliciosa, sin el conocimiento ni ta autorización del usuario No se replica a si mismo como los virus reales, no hace copias de si mismo como los gusanos y suele propagarse a través de correo electrónico o descargas de archivos de internet. La carga útil de los troyanos varia mucho según los casos. Pueden robar contraseñas, infectar una computadora con un virus o incluso actuar como puerta trasera para espiar a los usuarios, registrando las pulsaciones de teclas y transmitiéndolas a un tercero a través de TCP/IP.

DEFINICION

Los troyanos pueden surgir en cualquier parte del sistema, pero no aparecen de forma espontánea ni se pueden propagar sin la intervención de algún usuario, ya que somos nosotros quienes introducimos físicamente este tipo de programas en el sistema, a través de cualquier medio transportable (disquetes, CDS) o de alguna conexión de red.

Los troyanos constituyen un alto riesgo por varias razones:

- "Se ejecutan de forma escondida, encubiertos en procesos legítimos de sistema. La mayoría de los programadores de troyanos escriben herramientas como sustitutos de utilidades de sistema de uso frecuente Al hacerlo, realizan dos suposiciones
- El usuario no va a mover ni suprimir el troyano. El usuario no se va a alarmar cuando vea su proceso en ejecución
- A menos que se adopten algunas medidas preventivas inmediatamente después de la instalación, los troyanos son difíciles de detectar. En computadoras de punto final los troyanos son archivos binarios compilados (ejecutables), por tanto no se puede examinar su código para detectar su código malicioso. .
- La detección de troyanos suele implicar el descubrimiento de cambios sospechosos en archivos de alguna unidad"

La mayoría de troyanos, como Back Orifice (B02K) utilizan plugins para implementar la funcionalidad por módulos información del sistema, levantare un servidor FTP para transferencia de archivos con todos los permisos de acceso a todas las unidades, levantarle un pequeño servidor web para bajarse sus archivos capturar la pantalla de la victima para fisgonear lo que está haciendo en ese momento, robar sus contraseñas, reiniciar la máquina, apagarla, bloquear o mover el cursor del mouse, ejecutar comandos y programas enviar mensajes de sistema personalizados por el intruso, configurar el acceso a la maquina victima, apagar el monitor, tomar el control remoto de su pantalla, cerrar ventanas, abrir y cerrar sus unidades de CD-ROM, entre muchas otras monerias que se le puedan ocurrir al programador del troyano

MEJORES PRACTICAS PARA EL CONTROL DE TROYANOS

La siguiente lista, recomienda qué hacer para tener las mejores prácticas en la protección contra troyanos:

- Guarde la etiqueta (en donde se mete, ya sea internet o a cualquier otro lugar), Fijese dónde se mete (utilice certificados digitales en los lugares que visita, que le aseguren que es un sitio seguro, esto se puede observar en el navegador, en una pantalla que aparece al establecer

comunicación con los navegadores donde nos indica si es o no un lugar conocido y certificado). De lo contrario, se asume el riesgo de acceder a lugares "desconocidos".

- Ya que la internet se maneja a través de direcciones, es recomendable que para guardar el anonimato y no ser presa tan fácil de aquellos que siguen la actividad de los demás (personas dedicadas al marketing, intrusos), se recomienda que la información que envía el navegador sea mínima, esto para proteger la identidad, dirección y toda aquella información que le pueda ser útil a los espías y que con la recolección de ésta, intenten aprovecharse del conocimiento sobre nosotros y sobre nuestras vulnerabilidades. Por eso se recomienda el uso de un servidor intermedio al que se dirija una petición de determinada página. El servidor de la URL solicitada no puede saber nada sobre las personas que visitan sus páginas. Un ejemplo de servidor intermedio es anonimazer.com el cual funciona de manera sencilla, se accede a el y después sólo es necesario introducir la dirección de la página Web solicitada para pasar inadvertido.
- Use programas detectores de troyanos como The cleaner" o software antivirus que tengan la capacidad de reconocer este código (la mayoría de los antivirus actuales tiene en sus búsquedas este tipo de código como punto a verificar su existencia u comportamiento).

En general, el uso adecuado (realizar actualizaciones, uso recomendado) de antivirus, dará una idea más clara de la actividad en cuanto a puertas traseras en nuestro sistema. Finalmente, visitar el sitio del fabricante del sistema operativo usado en busca de parches de seguridad.

SPYWARE Y ADWARE

DESCRIPCION Y EVALUACION

"Dentro de las plagas de Internet, como el correo basura o spam, podemos mencionar otras, como los programas de publicidad no deseada o adware y los programas espías o spyware. Ambos tienen su origen en los programas de dominio público o shareware."

Con esta modalidad, programadores independientes o empresas comerciales invitan a utilizar sus programas por un periodo de tiempo o con ciertas limitaciones en las prestaciones, a los efectos que el usuario del programa, en caso de encontrarlo útil, pague por la utilización de este.

Los usos" que se les podría dar a los spywares son variados, todos en contra de los intereses y privacidad de los internautas.

2.1.2. Marco referencial sobre la problemática de investigación.

2.1.2.1. Antecedentes investigativos.

En lo que respeta a la temática específica sobre el: “Amenazas, Vulnerabilidades y su Incidencia en el Sistema Informático de La red Corporación Nacional de Telecomunicaciones CNT E.P Los Ríos.”, existen varios trabajos de investigación realizados por otros profesionales e instituciones, siendo estos los siguientes:

La tesis, denominada: “UNA PROPUESTA DE SEGURIDAD EN LA INFORMACION CASO SYSTEMATICS DE MEXICO S.A.”. Trabajo realizado por el Lic. Fernando Bugarini Hernandez Año 2007. En este estudio se señala: “Los ataques a computadoras en red pueden causar perdidas de dinero, tiempo, productos, reputación, información confidencial, y datos sensibles , sin embargo , estos pueden ser prevenidos”.

La tesis, denominada: “ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL AREA TECNICA DE REPARACION E INSTALACION DE LA CORPORACION NACIONAL DE TELECOMUNICACIONES "CNT EP" DE LA CIUDAD DE BABAHOYO..”. Trabajo realizado por el Ing. Crysthian Geovanny Villamar Silva Año 2021. En este estudio se señala: “Las normativas de seguridad de la información por los controles que estás se han diseñado para reducir los impactos como mejorar la seguridad deben venir apegadas a políticas que son normativas también pero de nivel más aterrizado la realidad de la organización, estás políticas en el caso de una empresa tan grande como CNT EP, deben también desplegarse a los territorios para ser cumplidas por todo el personal técnico hasta la persona que

utiliza el sistema más mínimo o cuenta con una computadora conectada a la red local".

La tesis, denominada: "Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013". Trabajo realizado por el CPA Moscaiza Moncada, Omar Israel. Año 2018. En este estudio se señala: "La validación del presente modelo de Sistema de Gestión de Seguridad de la Información ha conseguido elaborar el Plan Estratégico de Seguridad de la Información de la CAC, producto de haber alineado los resultados de madurez de los dominios tanto de las normas ISO 27001:2013, ISO 27002:2013 y los resultados del análisis de brechas. En base a los valores obtenidos se pudieron determinar los planes de seguridad pertinentes".

En la tesis titulada: "Seguridad en informática (Auditoria de Sistemas).". Trabajo realizado por: Luis Daniel Alvarez Basaldua. Año 2005. En este estudio concluye: " Actualmente, las organizaciones modernas que operan o centran gran parte de su actividad en el negocio a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades; en este sentido, cobra especial importancia el hecho de que puedan contar con profesionales especializados en las nuevas tecnologías de seguridad que implementen y gestionen de manera eficaz sus sistemas..".

2.1.2.2. Categorías de análisis.

2.1.3. Postura teórica.

Nos identificamos con las teorías propuestas en los modelos de gestión de Seguridad de La información:

Mark T. Abene.- Su enfoque principal era explorar sistemas de telecomunicaciones, sistemas operativos de minicomputadoras y mainframe y redes de datos de paquetes a gran escala. El eventual declive de la LOD hacia

finales de la década de 1980 en gran parte debido a la fragmentación y la disidencia dentro del grupo, junto con el enjuiciamiento legal de un puñado de sus miembros, hizo que Abene se alineara cada vez más con un grupo local de hackers prometedores, que llegaron a ser conocidos como los Maestros del Engaño (MOD)

Jon Callas. - Callas ha declarado que las empresas de tecnología son una amenaza mayor para la privacidad que el gobierno. Sus puntos de vista se derivan de la agrupación masiva de datos personales de las grandes tecnológicas para la publicidad y la polarización dentro de Silicon Valley. Si bien algunas empresas están comprometidas con la privacidad, muchas más obtienen sus ingresos de la venta de datos de usuarios. Callas ha declarado que, si el mercado publicitario se desacelera, las empresas que protegen los datos de sus usuarios son las más aisladas de los daños

De Adalberto Chiavenato. - Se focalizan en seis vertientes: la admisión de personas, los cursos de capacitación, monitoreo, control, sistemas de información y bases de datos informáticos.

De Beer.- Cuatro campos diferentes pero que poseen las mismas denominaciones en cuanto a las políticas correspondientes.

En cuanto al manejo propio de la Seguridad de la Información de la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos , nos apegamos a la regulación establecida por la Superintendencia de Telecomunicaciones, dentro de la clasificación de las Empresas de Telecomunicaciones. Debiendo cumplir con las normas establecidas por la Ley Orgánica de Empresas publicas y del sector de las telecomunicaciones.

2.2. Hipótesis.

2.2.1. Hipótesis general.

Potenciando el sistema de seguridad informática en la Corporación Nacional de Telecomunicaciones CNT EP Agencia Los Ríos, mejorará la productividad de la empresa.

2.2.2. Subhipótesis o derivadas.

- Determinado un sistema de detección de amenazas la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos. Mejora su productividad.

- Identificada las necesidades y exigencia del sistema actual de detección de amenazas se optimizo el sistema y cumple con las expectativas que los usuarios requieren mejorando la calidad en la atención Corporación Nacional de Telecomunicaciones CNT EP Los Ríos.

- Diseñado el plan de capacitación y de mejora continua sobre el sistema de detección de amenazas y debilidades de los sistemas informáticos de la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos. Se perfecciono el perfil profesional del talento Humano.

2.2.3. Variables.

- **Variable dependiente.**
  - Seguridad de la información
- **Variable independiente.**
  - Satisfacción del cliente

CAPÍTULO III.- RESULTADOS DE LA INVESTIGACIÓN.

3.1. Resultados de investigación.

3.1.1 Pruebas estadísticas aplicadas.

La población o universo de esta investigación se encuentra constituida por el personal total del personal de la CNT EP Agencia Los Ríos, los cuales son un total de 103 personas, así como los clientes 20000, personas quienes son los directamente beneficiados en el proceso productivo de la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos.

Para el caso del Personal de la agencia Los Ríos se aplicó el 100% de la población para la aplicación del instrumento, siendo el total de la muestra el de ciento tres objetos de observación.

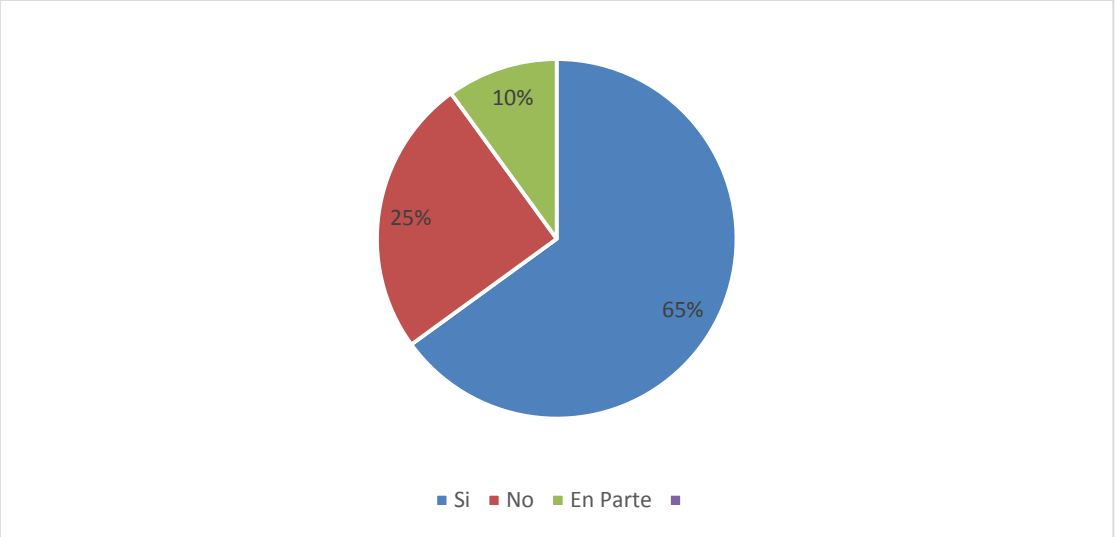
Los otros actores lo constituyen los clientes, para este caso se aplicó una fórmula para poblaciones finita, a fin de obtener la muestra, obteniéndose un total de 202 objetos de observación.

3.1.2 Análisis e interpretación de datos

Encuesta servidores

¿Cree usted que las instalaciones físicas de CNT EP son las adecuadas para desempeñar bien su labor?

Alternativa	Frecuencia	Porcentaje
Si	67	65%
No	26	25%
En Parte	10	10%
Total	103	100%



Fuente: Investigador

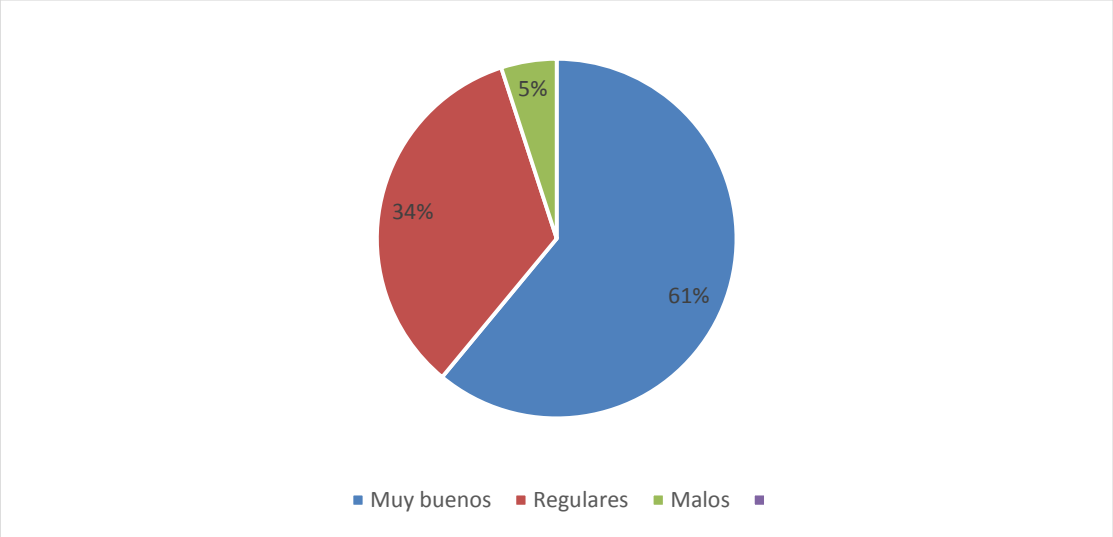
Análisis. – Al consultar el “Cree usted que las instalaciones físicas de CNT EP son las adecuadas para desempeñar bien su labor”, se determina que el 65% cree que sí, el 25% cree que no; el 10% cree que en parte.

Interpretación. – De acuerdo con los resultados obtenidos en esta pregunta, se determina que existe un alto índice de aceptación de los empleados de la

empresa, esto es positivo porque demuestra fidelidad hacia la organización de parte de sus integrantes.

¿Cómo califica usted los recursos materiales y suministros con los que cuenta para brindar el servicio al cliente?

Alternativa	Frecuencia	Porcentaje
Muy buenos	63	61%
Regulares	35	34%
Malos	5	5%
Total	103	100%



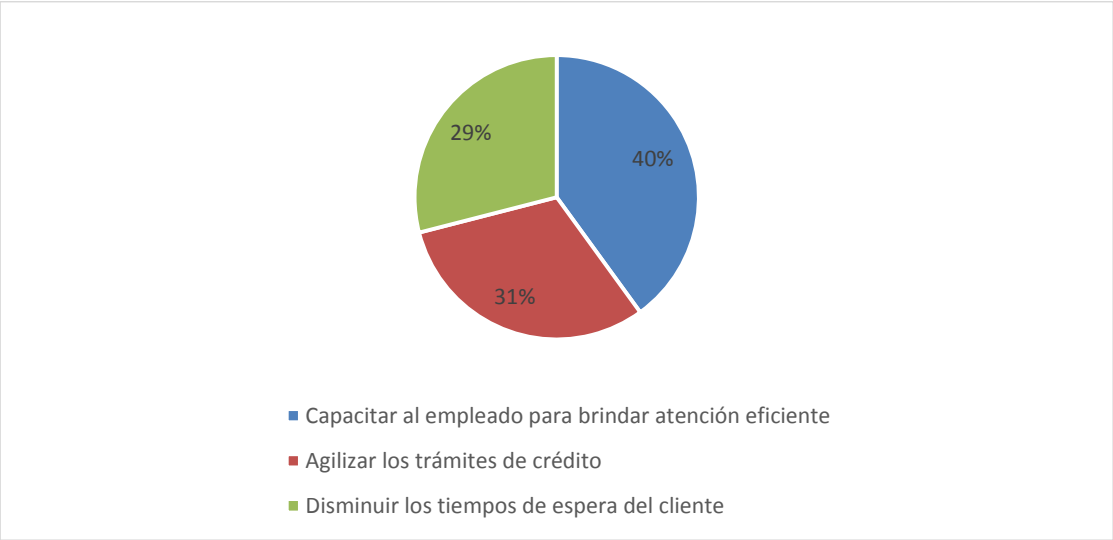
Fuente: Investigador

Análisis. – Al consultar el "¿Cómo califica usted los recursos materiales y suministros con los que cuenta para brindar el servicio al cliente?", se determina que el 61% cree que son muy buenos el 34% cree que son regulares; el 5% cree que son malos.

Interpretación. – De acuerdo con los resultados obtenidos en esta pregunta, se determina que existe un alto índice de conformidad de los empleados de la empresa, sin embargo, las objeciones presentadas también constituyen un número importante que debe tomarse en cuenta para mejorar los recursos que provee la empresa a sus colaboradores.

¿Cuál considera usted que es la mejor estrategia para mejorar el servicio en la CNT EP?

Alternativa	Frecuencia	Porcentaje
Capacitar al empleado para brindar atención eficiente	41	40%
Agilizar los trámites de crédito	32	31%
Disminuir los tiempos de espera del cliente	30	29%
total	103	100%



Fuente: Investigador

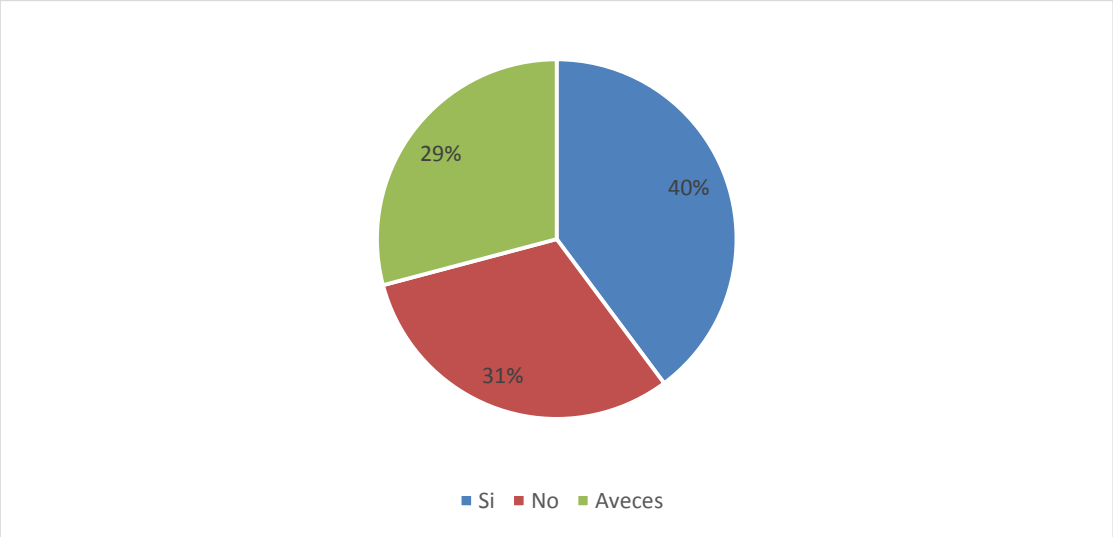
Análisis. – Al consultar el "¿Cuál considera usted que es la mejor estrategia para mejorar el servicio en la CNT EP?", se determina que el 40% cree que Capacitar al empleado para lograr una atención eficiente el 31% cree que Agilizar los tramites de crédito; el 30% cree que disminuir los tiempos de espera de los clientes.

Interpretación. – De acuerdo con los resultados obtenidos en esta pregunta, se determina que existe un alto índice de inconformidad de los empleados en cuanto a las capacitaciones recibidas y que considerando la relación entre la

segunda y tercera opción que se refieren a los tiempos de atención se debe priorizar alternativas que se enfoquen a reducir los tiempos de atención.

¿Cree usted que el tiempo que utiliza para la prestar un servicio en la CNT EP es el adecuado?

Alternativa	Frecuencia	Porcentaje
Si	45	44%
No	32	31%
A veces	26	25%
total	103	100%



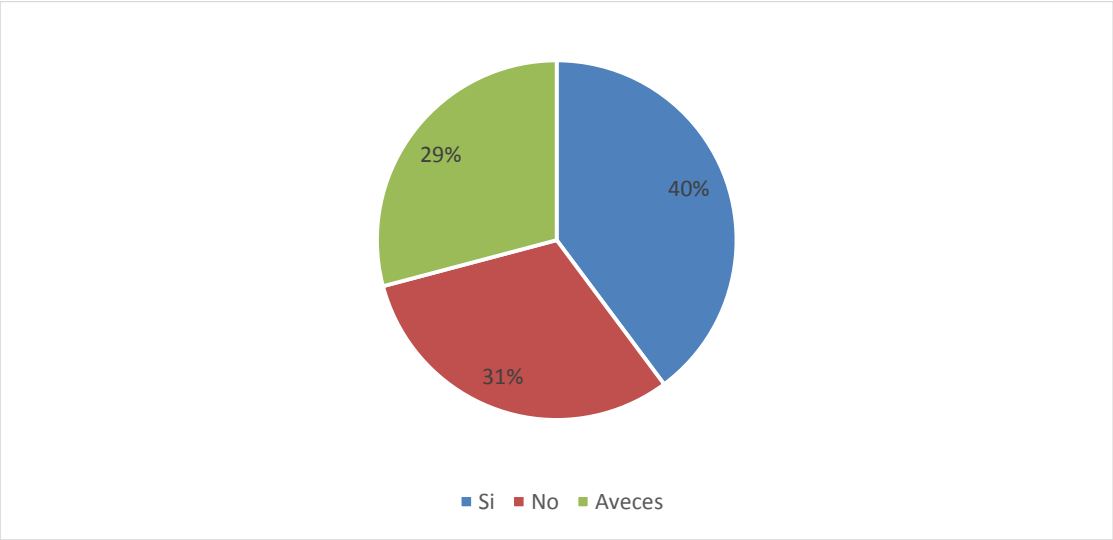
Fuente: Investigador

Análisis. – Al consultar el "¿Cree usted que el tiempo que utiliza para la prestar un servicio en la CNT EP es el adecuado?", se determina que el 44% cree que si, el 31% cree que no; el 25% cree que a veces.

Interpretación. – Los resultados obtenidos en esta pregunta, determinan que existe un alto índice de preocupación de los empleados por los tiempos de atención y que considerando la relación entre la segunda y tercera opción se debe priorizar alternativas que se enfoquen a reducir los tiempos de atención lo cual es consistente con el análisis de la pregunta anterior.

¿Cuál considera usted que es la mayor causa de quejas en el servicio por parte de los clientes?

Alternativa	Frecuencia	Porcentaje
Falta de agilidad en la atención	19	18%
Tramites de crédito complicados	49	48%
Falta de capacitación del personal que atiende al cliente	35	34%
total	103	100%



Fuente: Investigador

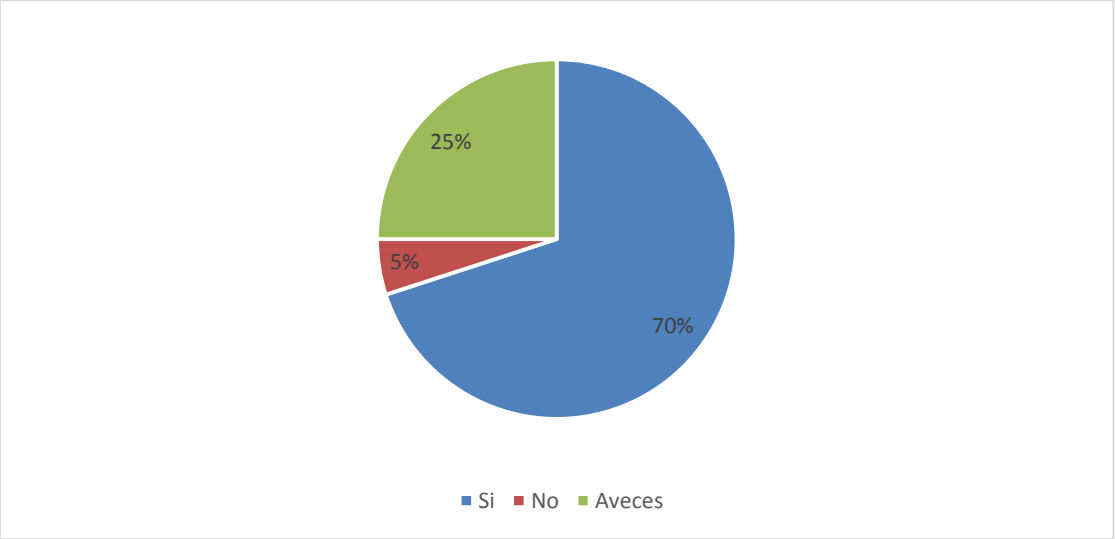
Análisis. – Al consultar el "¿Cuál considera usted que es la mayor causa de quejas en el servicio por parte de los clientes?", se determina que el 18% cree que es la falta de agilidad en la atención, el 48% cree que Tramites de crédito complicados ; el 34% cree que Falta de capacitación del personal que atiende al cliente.

Interpretación. – Los resultados obtenidos en esta pregunta, muestran que el personal requiere de capacitación especifica en los procedimientos para ser

más agiles, así también debe existir una simplificación en lo procesos sin descuidar la seguridad de la información.

¿Considera usted que, mediante un programa de capacitación en Seguridad de la Información, permitirá mejorar el servicio de la institución?

Alternativa	Frecuencia	Porcentaje
Si	72	70%
No	5	5%
En Parte	26	25%
total	103	100%



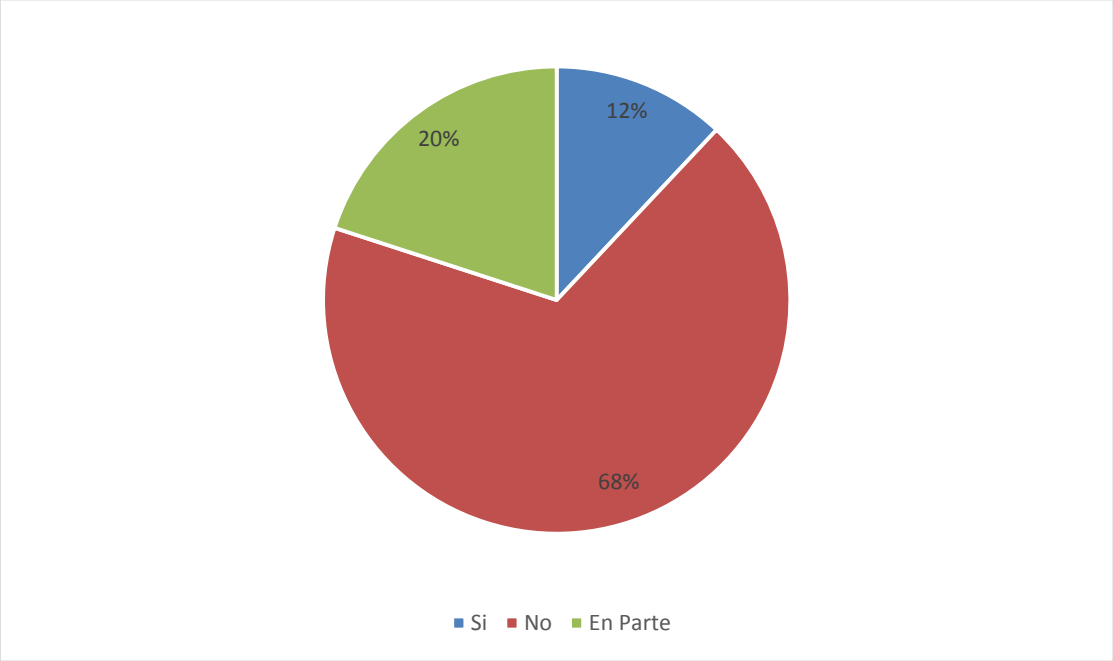
Fuente: Investigador

Análisis. – Al consultar el ¿Considera usted que, mediante un programa de capacitación en Seguridad de la Información, permitirá mejorar el servicio de la institución?", se determina que el 70% cree que sí, el 5% cree que no; el 25% cree que en parte.

Interpretación. – la perspectiva que nos presenta el resultado obtenido en esta pregunta nos deja claro el conocimiento de la importancia de la seguridad de la información para los servidores de la CNT EP , y la gran mayoría concuerda en que la capacitación es la mejor alternativa para solventar los problemas que se han presentado .

¿Considera usted que la remuneración que recibe por su labor es el adecuado respecto a la función que usted cumple?

Alternativa	Frecuencia	Porcentaje
Si	12	12%
No	70	68%
En Parte	21	20%
total	103	100%



Fuente: Investigador

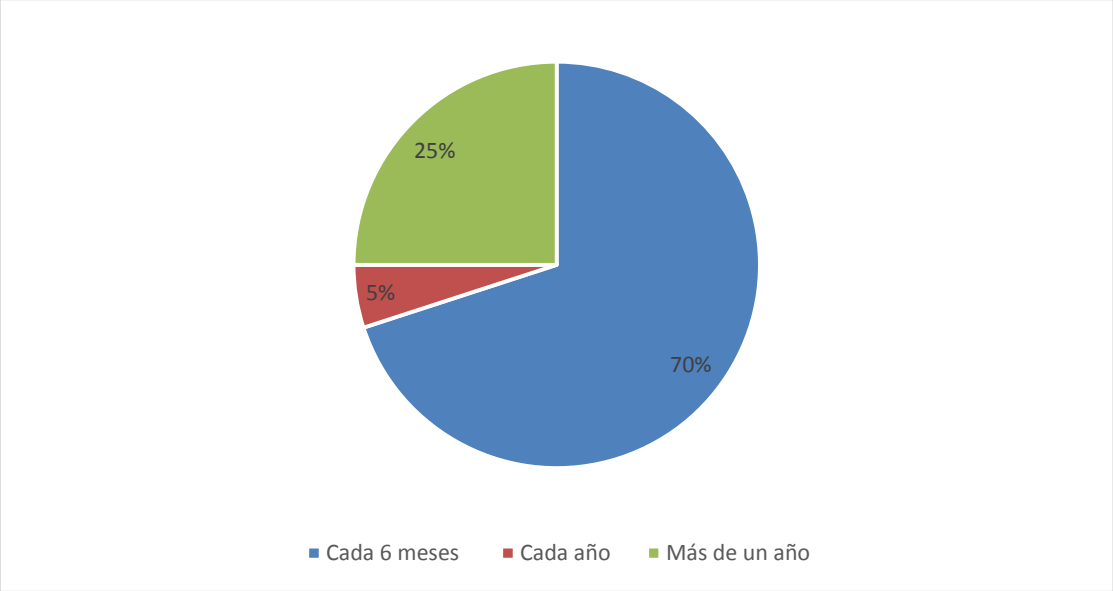
Análisis. – Al consultar el ¿Considera usted que la remuneración que recibe por su labor es el adecuado respecto a la función que usted cumple?", se determina que solo el 12% cree que sí, el 68% cree que no; el 20% cree que en parte.

Interpretación. – las respuestas obtenidas en esta pregunta son realmente alarmante por que hablan de un alto nivel de insatisfacción de los servidores,

los que realmente podría ser un riesgo potencial para la seguridad de la información de la empresa.

¿Cada qué tiempo recibe usted capacitación en los sistemas de seguridad de la información, por parte del departamento de capacitación de la CNT EP?

Alternativa	Frecuencia	Porcentaje
Cada 6 meses	72	70%
Cada año	5	5%
Más de un año	26	25%
total	103	100%



Fuente: Investigador

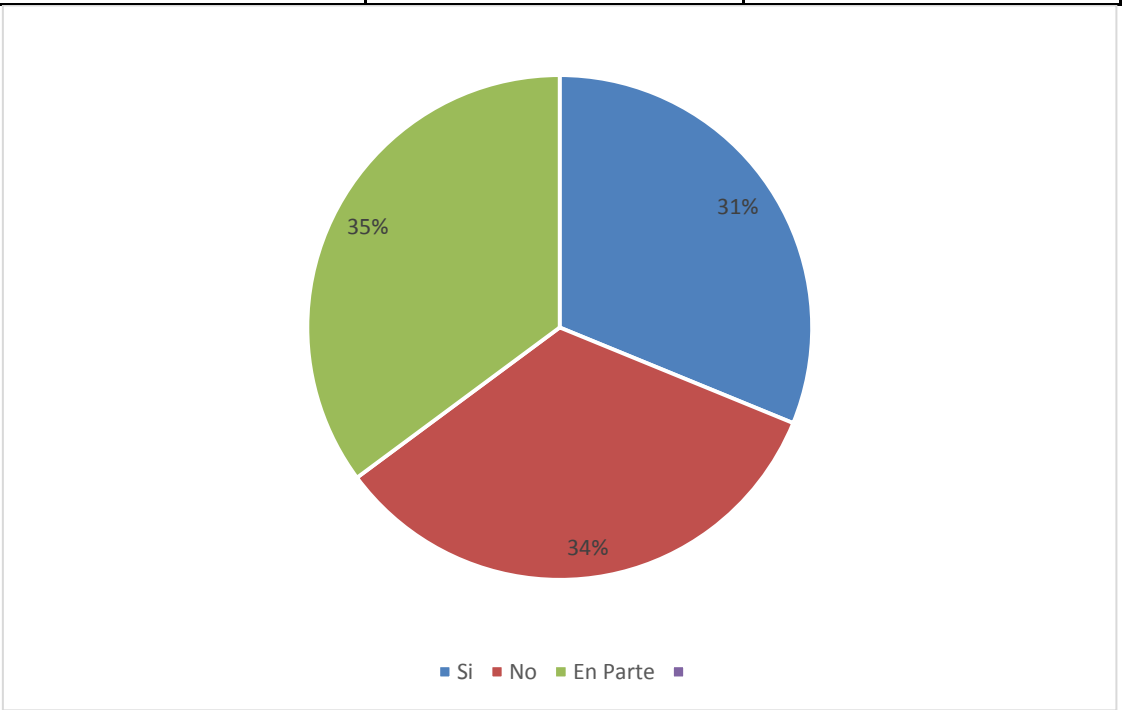
Análisis. – Al consultar el ¿Cada qué tiempo recibe usted capacitación en los sistemas de seguridad de la información, por parte del departamento de capacitación de la CNT EP?", se determina que el 70% recibe capacitaciones cada 6 meses, el 5% lo hacen cada año y el 25% recibe capacitaciones sobres seguridad de la información pasando más de un año.

Interpretación. – se evidencia que pese a que CNT EP invierten capacitaciones estas parecen no ser optimas en cuanto a su contenido no están alineadas a los requerimientos y realidad de la empresa.

Encuesta clientes

¿Al integrarse como cliente de la CNT EP se le facilito la información de manera rápida?

Alternativa	Frecuencia	Porcentaje
Si	63	31%
No	68	34%
En Parte	71	35%
Total	202	100%



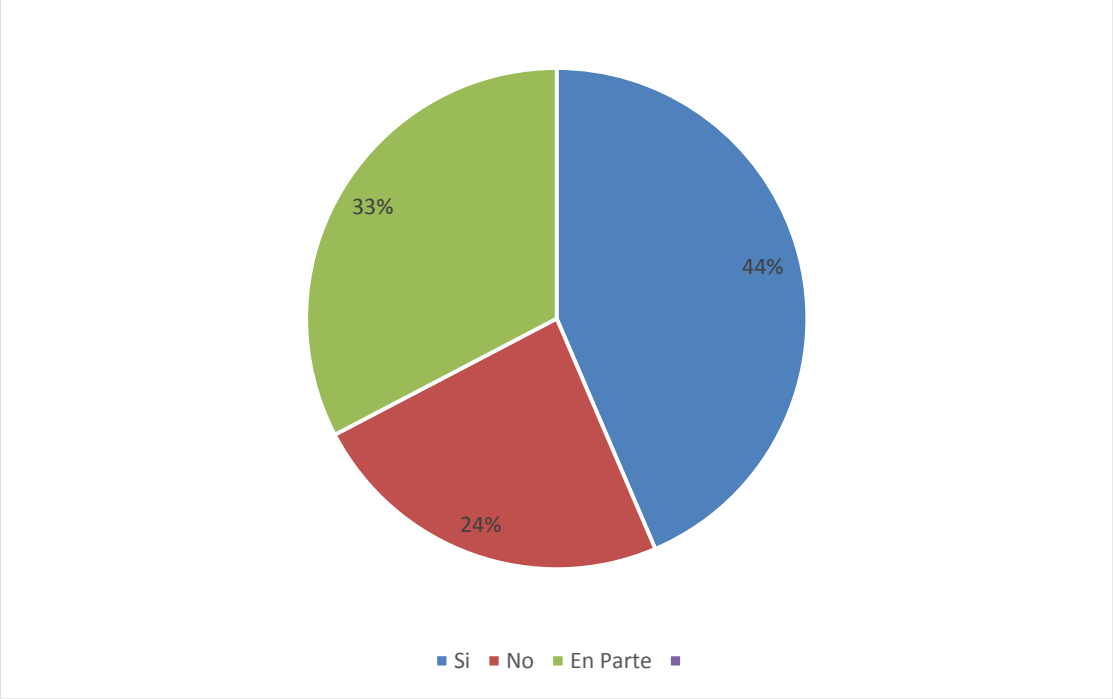
Fuente: Investigador

Análisis. – Al consultar el “Al integrarse como cliente de la CNT EP se le facilito la información de manera rápida”, se determina que el 31% cree que sí, el 34% cree que no; el 35% cree que en parte.

Interpretación. – De acuerdo con los resultados obtenidos en esta pregunta, se determina que existe un alto índice de inconformidad en cuenta a la atención al cliente que brinda la empresa de la empresa, esto es negativo porque afecta la relación de la marca CNT EP con los clientes.

¿Cree usted la información que se da a los clientes al momento de buscar un servicio en la CNT?

Alternativa	Frecuencia	Porcentaje
Si	88	44%
No	48	24%
En Parte	66	33%
Total	202	100%



Fuente: Investigador

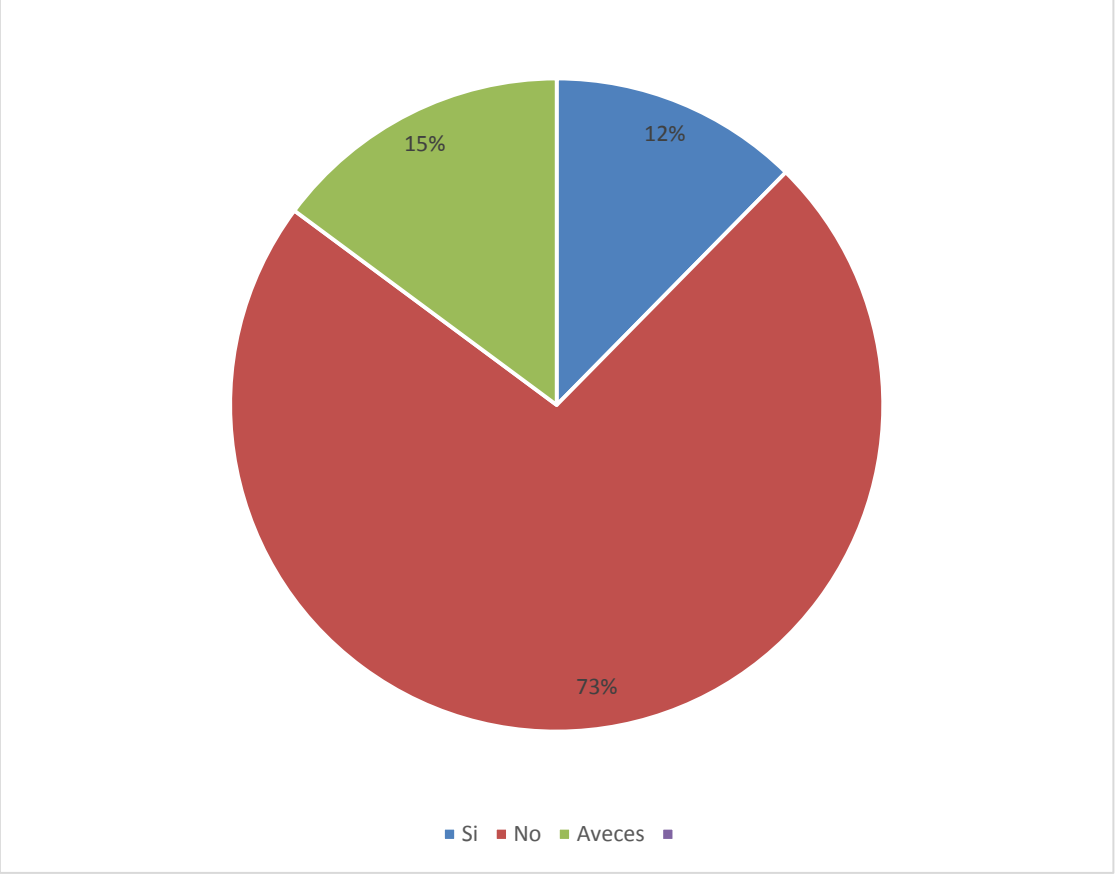
Análisis. – Al consultar el "¿Cree usted la información que se da a los clientes al momento de buscar un servicio en la CNT?", se determina que el 44% cree que sí, el 24% cree que no; el 33% cree que en parte.

Interpretación. – De acuerdo con los resultados obtenidos en esta pregunta, se determina que existe un mediano índice de conformidad en cuenta a la atención al cliente que brinda la empresa de la empra, esto es alarmante

porque indica falta de eficiencia afecta la relación de la marca CNT EP con los clientes.

¿Ha tenido algún inconveniente con el personal de atención al momento de solicitar algún servicio?

Alternativa	Frecuencia	Porcentaje
Si	25	12%
No	147	73%
A veces	30	15%
Total	202	100%



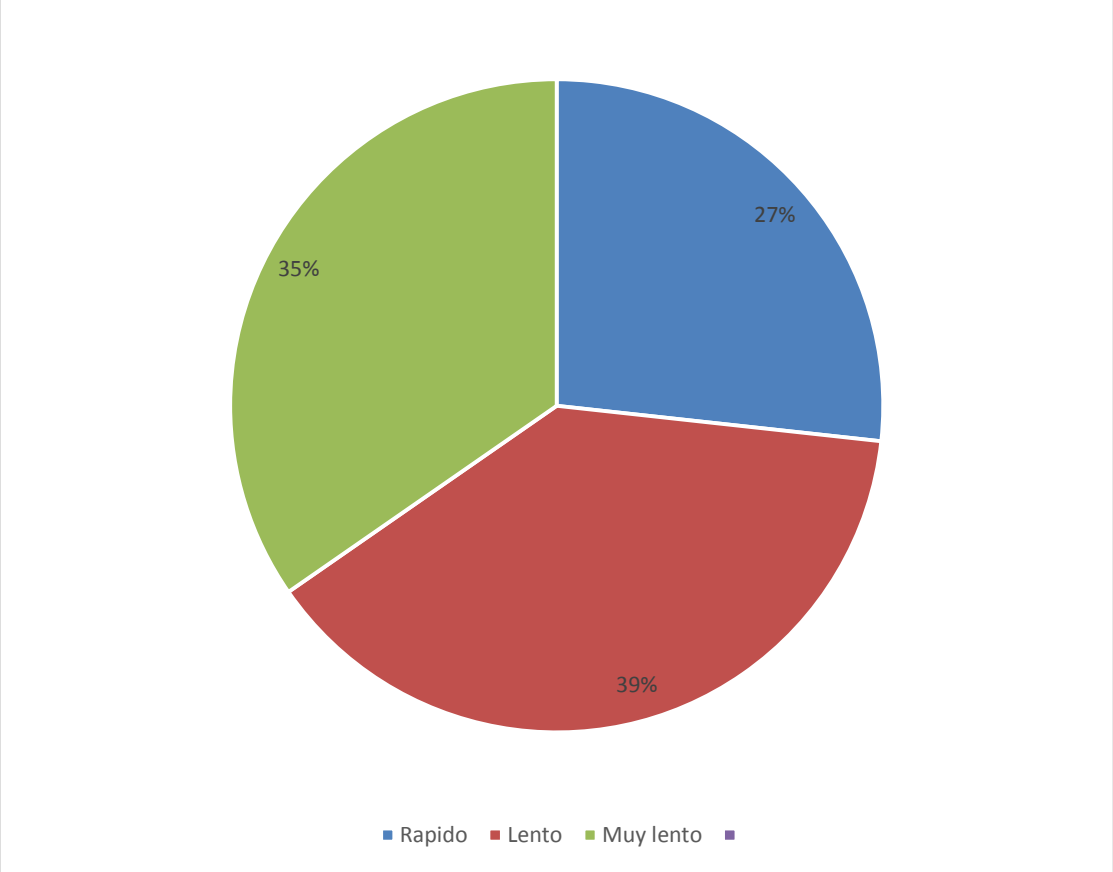
Fuente: Investigador

Análisis. – Al consultar el "¿Ha tenido algún inconveniente con el personal de atención al momento de solicitar algún servicio?", se determina que el 25% cree que sí, el 73% cree que no; el 15% a veces.

Interpretación. – De acuerdo con los resultados obtenidos en esta pregunta, se determina que existe un marcado índice de conformidad en cuenta a la atención al cliente que brindan el personal de la empra, esto es estimulante porque indica buen trato de los asesores CNT EP con los clientes.

¿Cómo considera usted que es la fluidez de los procesos para atender los requerimientos?

Alternativa	Frecuencia	Porcentaje
Rápido	54	27%
Lento	78	39%
Muy lento	70	35%
Total	202	100%



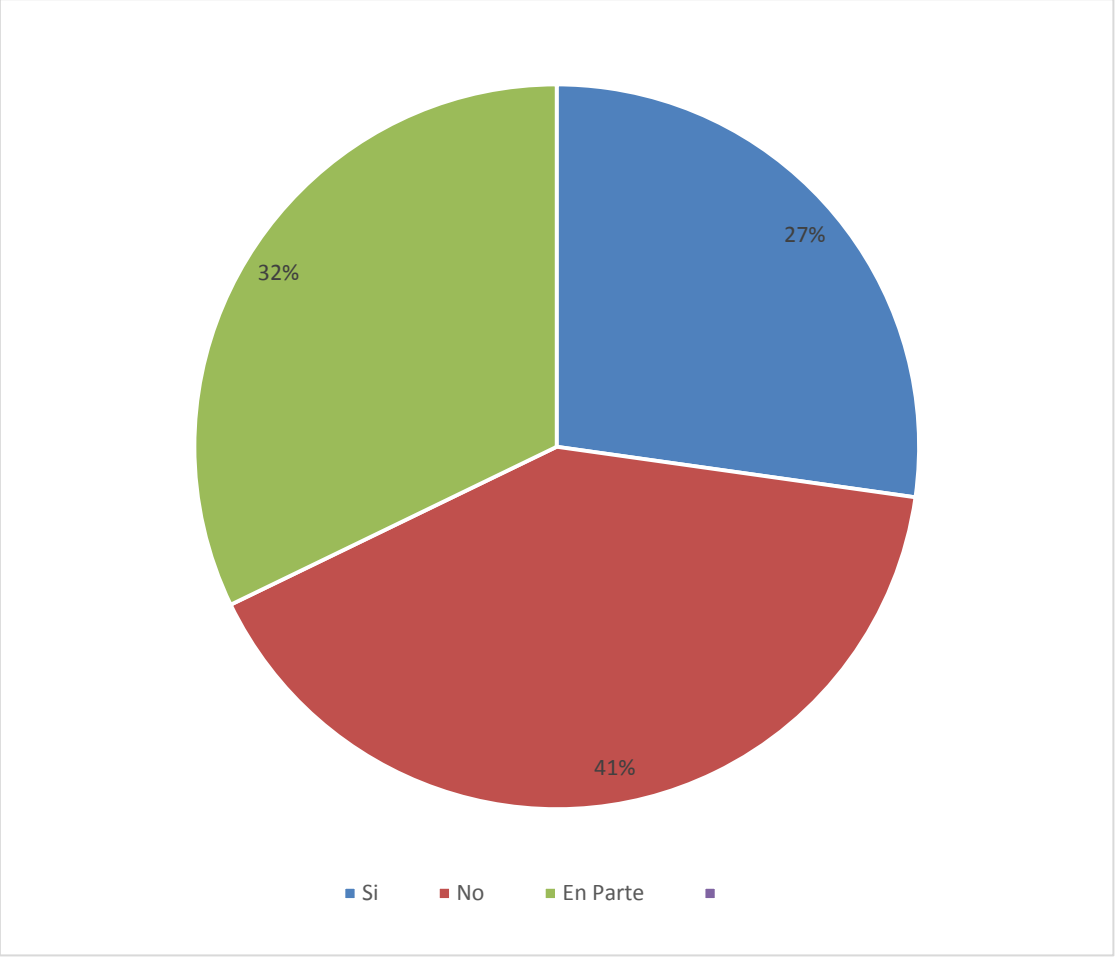
Fuente: Investigador

Análisis. – Al consultar el "¿Cómo considera usted que es la fluidez de los procesos para atender los requerimientos?", se determina que el 27% cree que es rápido, el 39% cree que es lento; el 35% cree que es muy lento.

Interpretación. – De acuerdo con los resultados obtenidos en esta pregunta, se determina que existe una mala percepción de los tiempos de respuesta a los requerimientos de los servicios que CNT EP ofrece a sus los clientes.

¿Cree usted que el tiempo que utiliza para la prestación de un servicio es adecuado?

Alternativa	Frecuencia	Porcentaje
Si	55	27%
No	82	41%
En Parte	65	32%
Total	202	100%



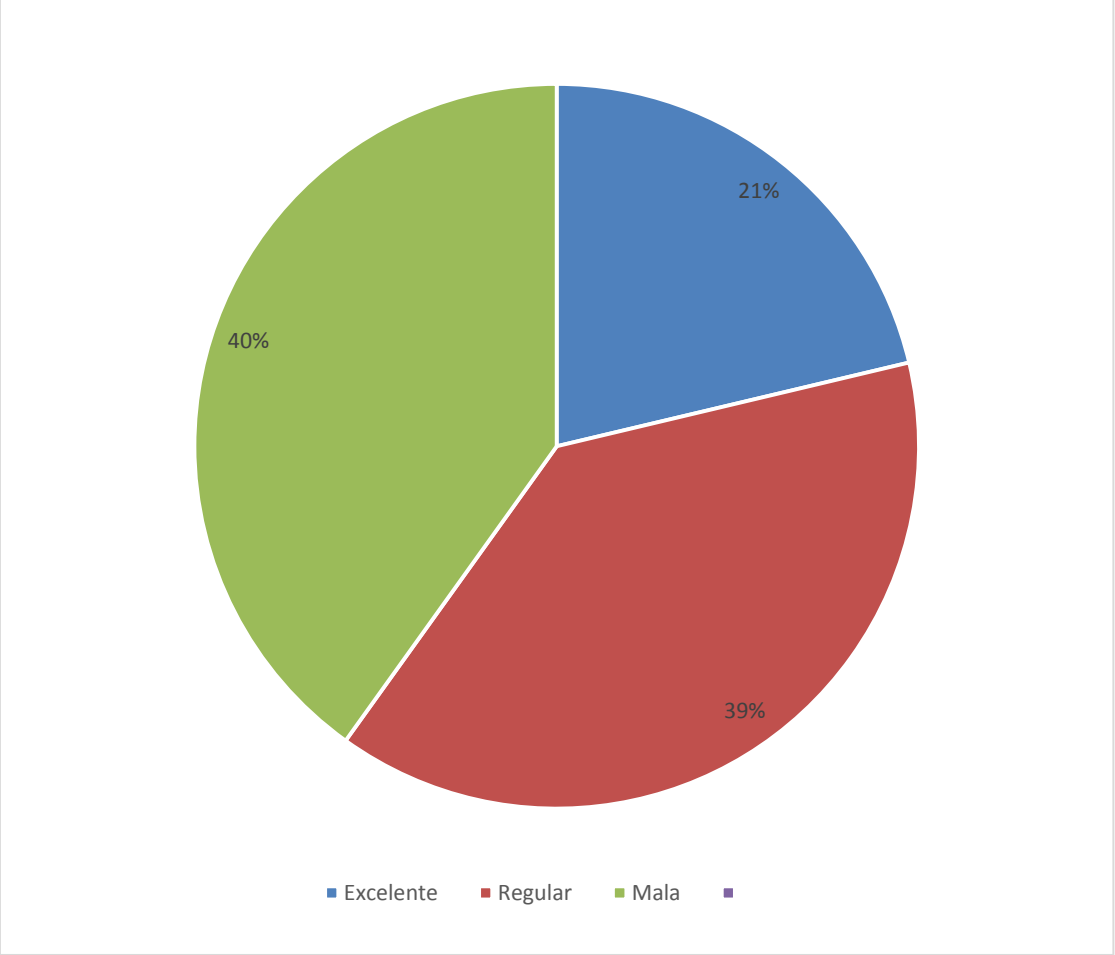
Fuente: Investigador

Análisis. – Al preguntar "¿Cree usted que el tiempo que utiliza para la prestación de un servicio es adecuado?", se determina que el 27% cree que sí, el 41% cree que no; el 41% cree que en parte.

Interpretación. – De acuerdo con los resultados obtenidos en esta pregunta, se determina que existe una mala percepción de los tiempos de respuesta a los requerimientos de los servicios que CNT EP ofrece a sus los clientes, esto guarda coherencia con la respuesta de las preguntas anteriores.

¿Qué calificación le da usted al servicio que recibe por parte del personal que lo atiende en la CNT EP?

Alternativa	Frecuencia	Porcentaje
Excelente	43	21%
Regular	78	39%
Mala	81	40%
Total	202	100%



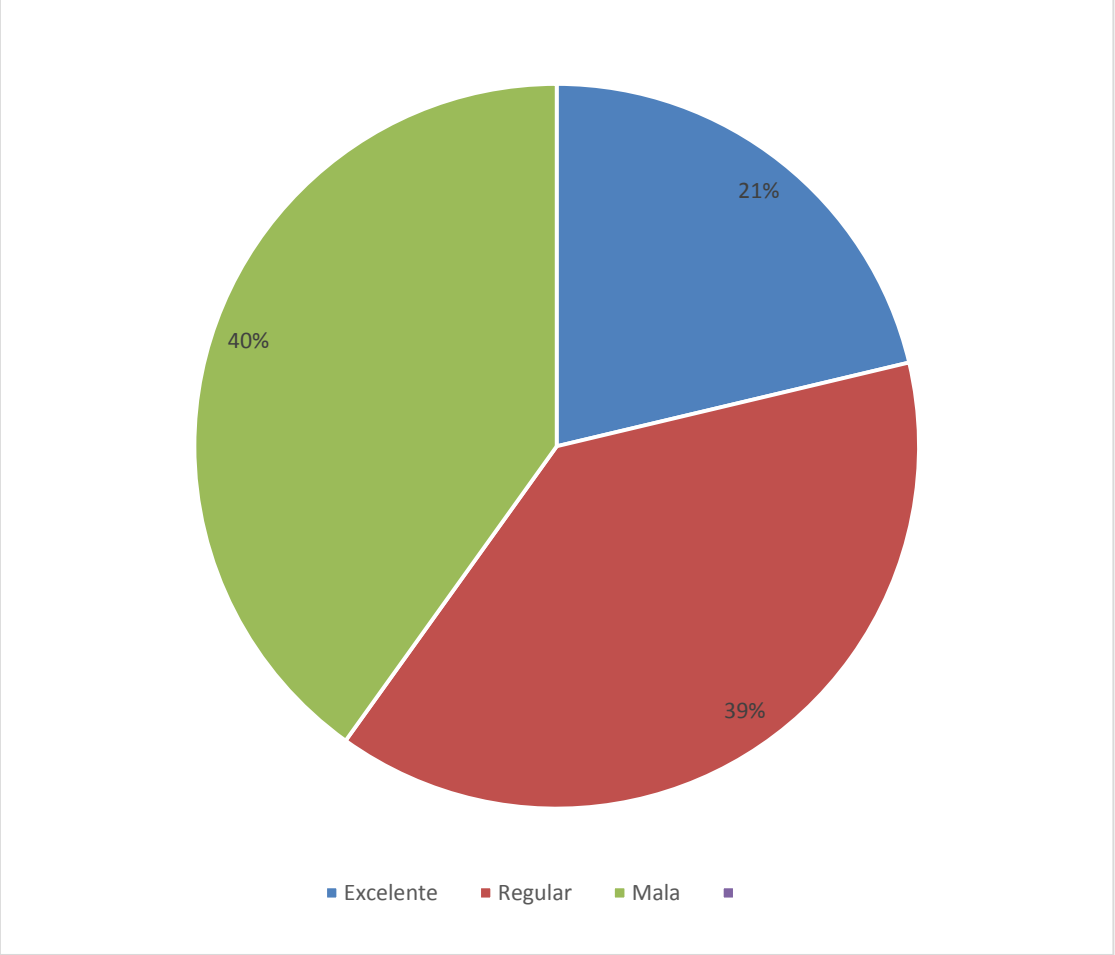
Fuente: Investigador

Análisis. – Al preguntar "¿Qué calificación le da usted al servicio que recibe por parte del personal que lo atiende en la CNT EP?", se determina que el 21% la considera excelente, el 39% cree que es regular; el 40% cree que es mala.

Interpretación. – De acuerdo con los resultados obtenidos en esta pregunta, se determina que existe una mala percepción de los servicios que CNT EP ofrece a sus los clientes, esto guarda coherencia con la respuesta de las preguntas anteriores.

¿Cómo califica la actitud con la que el personal que atiende al cliente ofrece información de los servicios de la CNT EP?

Alternativa	Frecuencia	Porcentaje
Excelente	80	40%
Regular	70	35%
Mala	52	26%
total	202	100%



Fuente: Investigador

Análisis. – Al preguntar “¿Cómo califica la actitud con la que el personal que atiende al cliente ofrece información de los servicios de la CNT EP?”, se determina que el 40% la considera excelente, el 35% cree que es regular; el 26% cree que es mala.

Interpretación. – De acuerdo con los resultados obtenidos en esta pregunta, se determina que existe una buena percepción de la actitud de los asesores aun cuando los servicios que CNT EP ofrece a sus los clientes no cumplen con las expectativas del cliente.

3.2. CONCLUSIONES ESPECIFICAS Y GENERALES.

3.2.1 ESPECIFICAS

Del estudio se puede determinar:

- Es una empresa Nacional, que esta direccionada a la prestación de servicios convergentes de telecomunicaciones y TICs en la Provincia de Los Ríos.
- EL personal que labora en la empresa, en su gran mayoría está dedicado a las labores de comercialización y producción y tiene sueldos acordes al mercado.
- La gestión del Talento Humano en CNT EP Los Ríos, se basa en conocimientos científicos administrativos, por lo cual la toma de decisiones es muy burocrática y afecta a su gestión.
- El talento humano que labora en esta empresa ha sido capacitado para el desarrollo de sus actividades específicas, sin embargo no se ajusta a los requerimientos de los clientes, por lo cual no existe eficiencia y eficacia en el desarrollo de sus actividades.
- El personal en un alto índice desea tener capacitación en el área de seguridad de la información, esto porque consideran que es el mejor campo de acción en la empresa y se controlaría de mejor manera las amenazas y se mitigarían los riesgos.

- El personal que labora en la CNT EP Los Ríos está de acuerdo con la aplicación de sistemas de seguridad de la información, porque consideran que la misma va a ayudar a realizar cambios en la gestión del Talento humano y por ende la rentabilidad va a aumentar en beneficio de las personas que están vinculadas de manera directa.

3.2.2 GENERAL

Se ha determinado que la investigación ha permitido identificar las debilidades de la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos Seguridad de la Información, su relación con la gestión del Talento Humano, considerando capacitación y atención al cliente.

3.3 RECOMENDACIONES ESPECIFICAS Y GENERALES

3.3.1 ESPECIFICAS

Las recomendaciones que se proponen en la investigación son:

- Que los directivos y empleados se capaciten en las normas ISO-27001, gestión del talento humano, servicio al cliente y técnicas de negociación para que la toma de decisiones permita aumentar la rentabilidad de este recurso de acuerdo a la potencialidad de cada uno de ellos.
- Que al personal se le reconozca el sueldo más los beneficios de Ley, para que este comprometido con los objetivos de la organización y busque constantemente elevar el volumen de ventas en beneficio de propietarios y empleados de la empresa negocio.
- Que se rote al personal, sobre todo a aquellos que desean insertarse en el campo de las ventas, dándoles la oportunidad de recibir los beneficios de sueldos más comisiones, esto permite fidelidad con la organización y compromiso de lograr metas y objetivos de la misma.
- Sugerir a las autoridades de la Facultad que se realice por medio del departamento de Vinculación con la sociedad, capacitación en gestión del normas ISO-27001, talento humano, servicio al cliente y técnicas de negociación para los pequeños empresarios de la ciudad de Babahoyo.

3.3.2 GENERAL

Que las debilidades del sistema de Seguridad de la Información de la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos, sirva para proponer alternativas que permita convertirlas en fortalezas que ayudara a competir por el mercado de la provincia de Los Ríos con empresas que ofrecen el mimo tipo de servicio en la localidad.

CAPITULO IV. PROPUESTA TEÓRICA DE APLICACIÓN.

4.1. Propuesta de aplicación de resultados.

4.1.1. Alternativa obtenida.

Plan de capacitación en la Seguridad de la Información basados en los sistemas de gestión ISO 27001 e impacto en la gestión del talento humano de la empresa Corporación Nacional de Telecomunicaciones CNT EP Los Ríos.

4.1.2 Alcance de la alternativa obtenida.

Se propone implantar un plan de en la Seguridad de la Información basados en los sistemas de gestión ISO 27001 e impacto en la gestión del talento humano de la empresa Corporación Nacional de Telecomunicaciones CNT EP Los Ríos, que permita dirigir de manera correcta al personal que labora en esta empresa, que permita mejorar los niveles de servicio y por ende la rentabilidad en base al compromiso de cada una de las personas que laboran en la misma, desempeñándose con eficiencia y eficacia.

El plan de capacitación se sustenta en la Detección de Necesidades de Capacitación (DNC) del personal en las áreas de ventas, atención al público, técnica de operaciones; en el caso de los directivos la capacitación debe estar en relación con la toma de decisiones en base concepciones técnicas de la ciencia administrativa.

Este plan de Capacitación es dirigido Servidores y obreros de la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos, se enfoca a la inducción (Onboarding) del actual personal, así como considerar la formación profesional del nuevo personal que a futuro ingrese a laborar.

4.1.2 Aspectos básicos de la alternativa.

Antecedentes

La empresa Corporación nacional de Telecomunicaciones Los Ríos está situada en la ciudad de Babahoyo, se dedica a proveer servicios convergentes de telecomunicaciones y TICs, tiene en el mercado más de 10 años, manteniendo una clientela que demuestra fidelidad, actualmente laboran en la misma 103 personas.

La gestión de la empresa está a cargo de sus directivos, los cuales tienen una formación en el área administrativa y la toma de decisiones se lo hace en base a la experiencia adquirida en los años al frente de la misma, pero esto si afecta a la rentabilidad de la organización por la lentitud en la toma de decisiones debido a los niveles burocráticos.

Considerando la fidelidad de los clientes, los propietarios del negocio se han despreocupado de la capacitación personal y de las personas que laboran en la empresa, motivo por el cual hay un estancamiento en ventas y no existe crecimiento de clientes, así como el compromiso de los empleados con la organización económica.

Justificación

La presente propuesta es de mucha importancia, porque va a permitir por medio de la capacitación elevar la productividad económica de la organización y el compromiso de los empleados con el negocio, así como la gestión administrativa de la empresa mejorara.

La propuesta aquí descrita, donde el punto principal son las capacitaciones al personal involucrado en la empresa, permitirá convertir las debilidades en fortalezas, relacionando a empleadores y empleados por los mismos objetivos, esto beneficiará a las dos partes vinculadas en el negocio.

4.2-Objetivos

4.2.1- Objetivo.

Mejorar el sistema de seguridad informática en la Corporación Nacional de Telecomunicaciones CNT EP Agencia Los Ríos para lograr aumentar la productividad de la empresa.

4.2.2- Objetivos específicos.

- Capacitar al personal de la empresa en los sistemas de detección de amenazas y la seguridad informática.
- Relacionar al Personal con exigencias actuales de la CNT EP para diseñar adecuadamente estrategias de seguridad informática.
- Retroalimentar la capacitación, después de evaluar al personal involucrado en la empresa de manera directa.

4.3- Estructura general de la Propuesta

4.3.1- Titulo.

Plan de mejoramiento en la gestión del talento humano de la Corporación Nacional de Telecomunicaciones CNT EP Los Ríosciudad de Babahoyo.

4.3.2- Componentes.

Capacitación para los empleadores y empleados, en:

Capacitación 1

- finalidad y el alcance de ISO 27001
- Términos y definiciones clave
- La estructura de ISO 27001
- Una descripción general de los requisitos de las cláusulas de ISO 27001 Procesos claves en la gestión del Talento humano

- Políticas de firewall alineadas con el ISO 27002
- Gestión de comunicaciones y operaciones
- Responsabilidades y procedimientos de operación.
- Documentación de los procedimientos de operación.
- Gestión de cambios.
- Segregación de tareas.

- Separación de los recursos de desarrollo, prueba y operación.
- Gestión de la provisión de servicios por terceros.
- Provisión de los servicios
- Supervisión y revisión de los servicios prestados por terceros.
- Gestión del cambio en los servicios prestados por terceros.
- Planificación y aceptación del sistema.
- Gestión de capacidades.
- Aceptación del sistema.
- Protección contra el código malicioso y descargable.
- Controles contra el código malicioso.
- Controles contra el código descargado en el cliente.
- Copias de seguridad.
- Copias de seguridad de la información.
- Gestión de la seguridad de las redes.
- Controles de red.
- Seguridad de los servicios de red.
- Manipulación de los soportes.
- Gestión de soportes extraíbles.
- Retirada de soportes.
- Procedimientos de manipulación de la información. 10.7.4 Seguridad de la documentación del sistema.
- Intercambio de información.
- Políticas y procedimientos de intercambio de información.
- Acuerdos de intercambio.
- Soportes físicos en tránsito.
- Mensajería electrónica.
- Sistemas de información empresariales.
- Servicios de comercio electrónico.
- Comercio electrónico.
- Transacciones en línea.
- Información públicamente disponible.
- Supervisión.

- Registros de auditoría.
- Supervisión del uso del sistema.
- Protección de la información de los registros.
- Registros de administración y operación.
- Registro de fallos.
- Sincronización del reloj.

Capacitación 2

- Conocimiento del producto
- Orientación al mercado
- Orientación a la empresa
- Habilidades en ventas
- Administración de tiempos y territorios
- Problemas legales y éticos
- Tecnología
- Negociación de precios
- Efectividad de ferias comerciales
- Lectura de lenguaje cultural
- Manejo de ansiedad de las visitas de ventas
- Capacitación en el puesto
- Interacción con el cliente
- Comunicación entre compañeros

Capacitación 3

- Ofrecer ayuda de forma activa
- Actuar con rapidez ante inquietudes del cliente
- Hablar el idioma del cliente
- Empleo de un lenguaje positivo
- Personalizar el trato al cliente
- Demostrar profesionalidad
- Vigilar el índice de satisfacción
- Utilizar estándares de medición

- El cliente centro de la empres

4.4 RESULTADOS ESPERADOS DE LA ALTERNATIVA.

Los resultados que se esperan con la aplicación de la propuesta son:

- Formación teórica-practica que permite elevar la productividad económica de la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos**.**
- Mejorar la selección de proveedores con las que trabaja la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos ciudad de Babahoyo.
- Mejorar la toma de decisiones por parte de los directivos de la empresa, para mejorar la rentabilidad.
- Aumentar el número de clientes, por medio de una atención de calidad y calidez a los existentes.

Proceso financiero Principios:

Eficacia. – Optimizar los recursos buscando los mejores resultados.

Eficiencia. – Reducir los costos proporcionando excelentes resultados.

Economía. – Disponer los recursos en el momento adecuado, sin excesos para lograr el menos costo posible. Es importante que la empresa tenga como prioridad los principios de planeación, organización y evaluación de los recursos económicos – financieros para que de esta forma las decisiones que se tomen tengan una proyección y razón de ser.

Planificación. - En el momento que en la distribuidora se tiene que tomar grandes decisiones tales como: financiamiento, inversión, destinos de resultados estos no pueden ser objetos del azar. Para esto debe de analizarse:

- Los riesgos del negocio
- Posibles desviaciones.
- Históricos de información crediticia para el caso en el que se necesite.

- Anticiparse a las decisiones futuras.

Organización. - La información económica – financiera de la distribuidora deberá ser respaldada debidamente ordenada y llevada en un registro de contabilidad ya que esto permitirá llevar un diagnóstico constante de las actividades que se desarrollan y una proyección segura, evidenciando la evolución y facilitando la toma de decisiones.

La organización de los estados contables se constituye en un pilar importante para dar el seguimiento a la realidad económica y financiera. Se deberá llevar:

- Registro contable de las operaciones económicas.
- Elaboración de estados contables.
- Elaboración de informes.
- Facturación.
- Registros de facturas de compras.
- Control de bodegas.
- Pérdidas y ganancias
- Gestiones de cobros y deudas pendientes

Mediante ambos métodos analizaremos diferentes aspectos tales como el modelo de gestión administrativo, su talento humano, la atención a clientes, la seguridad de la información, entre otros que me permitirá desde este conocimiento particular ir hacia lo general y concluir con una propuesta específica que mejore el perfil profesional del talento humano de la Corporación Nacional de Telecomunicaciones CNT E.P Los Ríos.

Es imprescindible que la empresa de seguimiento a la información pasada y actual registrada a través de los estados contables para comparar lo que se ha desarrollado con lo planificado, teniendo un diagnóstico claro que permita evaluar el uso de los recursos y la eficiencia y eficacia con la que se han manejado.

Se considerará a las pérdidas y ganancias registradas como elemento importante para el objeto de análisis en el cual se deberá ser minucioso y realista contemplando que la acción es determinar cuáles han sido los resultados.

Este efecto de retroalimentación hay que tenerlo en cuenta ya que permitirá tener el conocimiento necesario para tomar acciones de prevención o corrección en las acciones posteriores.

Situación actual	Cambios esperados
• Los procesos de comercialización son lentos y generan malestar en los clientes. • La estructura organizacional no posee una gerencia local para coordinar y tomar decisiones de manera descentralizada. • El proceso de selección y	• Los procesos de comercialización son gestionados de manera oportuna, mediante la implementación de las fichas de gestión para cada área. • El cargo de Jefe financiero se enfoca directamente al aspecto financiero, mantiene un control de ingresos y

contratación del personal no tiene establecidos los parámetros a considerar, careciendo de un proceso de capacitación formal y la evaluación del personal en base a los resultados obtenidos. • No hay registro de evidencia de los inconvenientes administrativos y de ventas presentados en la empresa. • Se presentan problemas en la toma de pedidos, en su respectivo ingreso, en la entrega de los Servicios y en ocasiones en la integridad física del producto por incorrecta manipulación o embalaje. • Las quejas de los clientes no son atendidas por la empresa y son resueltas a criterio del trabajador.	gastos, monitoreo de indicadores y aspectos relacionados a la rentabilidad, mediante la ficha de gestión de las finanzas. • La gestión del recurso humano tiene definido el proceso de selección, capacitación y evaluación del personal, determinando las funciones a realizar en cada etapa mediante la implementación de la ficha de gestión. • La gestión del control interno permite efectuar auditoría interna a los diferentes departamentos, manteniendo un registro de los problemas presentados y de las acciones implementadas para mejorar y control de sus resultados. • La gestión de la logística detalla cada uno de los procesos y la forma correcta de realizarlos, determinando tiempos específicos para la toma de pedidos, ingreso y despacho de mercadería y entrega manteniendo la integridad física del producto. • La gestión del servicio al cliente mediante la

	capacitación del personal con respecto al trato al cliente, manejo de conflictos, búsqueda de soluciones y seguimiento post venta garantiza la satisfacción y fidelización del cliente.

Tabla 2. Comparativo situacional

. Cronograma del proyecto.

N°	ACTIVIDAD	AÑO 2022											
		FEBRERO				MARZO				ABRIL			
		SEMANAS				SEMANAS				SEMANAS			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Elaboración de Proyecto de Investigación												
2	Revisión e Informe del Director Del Proyecto												
3	Presentación del Proyecto y Aprobación Legal												
4	Sustentación del Proyecto												

Bibliografía.

Journals

DIARIO EL COMERCIO CNT dijo que sufrió ataque informático de 'alta sofisticación'

FUENTE.-

https://www.elcomercio.com/actualidad/negocios/cnt-ataque-informativo-hackeo-sofistificacion.html

FORBES Hackeo a CNT genera problemas en la facturación

FUENTE.-

https://www.forbes.com.ec/negocios/hackeo-cnt-genera-problemas-facturacion-n6763

FRED PIPER, Cyberworld Security-the Good, the Bad and the Ugly University of London, Egham, Surrey TW20 OEX, UK. 2006

FUENTE.-
https://academic.oup.com/comjnl/article-abstract/48/2/145/576620?redirectedFrom=fulltext

IAN S. WELCH AND ROBERT J. STROUD, Re-engineering Security as a Crosscutting Concern; School of Mathematical and Computing Sciences, Victoria University of Wellington, New Zealand. 2006
FUENTE.-
http://comjnl.oxfordjournals.org/cgi/content/abstract/46/5/578?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=&fulltext=information+security&searchid=1&FIRSTINDEX=0&resourcetype=HWCIT

ENGIN KIRDA AND CHRISTOPHER KRUEGEL, Protecting Users against Phishing Attacks, Technical University of Vienna Vienna, Austria. 2006

FUENTE.-

http://comjnl.oxfordjournals.org/cgi/content/abstract/49/5/554?maxtoshow=

&HITS=10&hits=10&RESULTFORMAT=&fulltext=ínformation+security&searchid=10&FIRSTINDEX=10&resourcetype=HWCIT

R. BENJAMIN, B. GLADMAN2 AND B. RANDELL, Protecting IT Systems from Cyber Crime, Visiting Professor, Imperial College, London, University College, London, University of Bristol, 13 Bellhouse Walk, Kingsweston, Bristol BS11 2 QUE, UK, Independent consultant, specializing in Information Security. Department of Computing Science. University of Newcastle, Newcastle upon Tyne NE1 7RU, UK. 2006

FUENTE -

http://comjnl.oxfordjournals.org/cgi/content/abstract/41/7/4297maxtoshow=&HITS=10&hits=10&RESULTFORMAT=&fulltext-information+security&searchid=1&FIRSTINDEX=20&resourcetype=HWCT

ALEXEI VERNITSKI, Can Unbreakable Mean Incomputable, Department of Electronic Systems Engineering, University of Essex, Colchester UK. 2006 FUENTE http://comjnl.oxfordjournals.org/cgi/content/abstract/49/1/108?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=&fulltextnf-information+security&searchid=1&FIRSTINDEX-20&resourcetype=HWCIT

Libros

ÁLVAREZ MARAÑÓN GONZALO; PÉREZ GARCÍA PEDRO PABLO, Editorial McGraw-Hill; 1" edición 28/09/2004. SEGURIDAD INFORMÁTICA PARA LA EMPRESA Y PARTICULARES

ASENSIO GONZALO, Editorial McGraw-Hill, 29 de Mayo de 2006, SEGURIDAD INFORMÁTICA PARA TODOS

CHARLES CRESSON, security policy expert and consultant Wood, CISA, CISSP, POLITICAS DE SEGURIDAD INFORMATICA - MEJORES PRÁCTICAS INTERNACIONALES 2005

MICROSOFT CORPORATION, 1 edición (09/2004). IMPROVING WEB APPLICATION SECURITY: THREATS AND COUNTERMEASURES.

ANDREWS, MIKE: WHITTAKER, JAMES A., addison-wesley febrero 2004 HOW TO BREAK WEB SOFTWARE FUNCTIONAL AND SECURITY TESTING OF WEB APPLICATIONS AN D WEB SERVICES, 2004

RAMOS VARON ANTONIO ANGEL; CARLOS MIGUEZ PÉREZ; FERNANDO PICOUTO RAMOS, Anaya Multimedia 1° edición (09/2004). PROTEGE TU PC

CHRIS MCNAB, Anaya Multimedia 464 p. 1º edición (09/2004), SEGURIDAD DE REDES

GARCÍA BLANCO JOSÉ MARÍA NAVARRO PABLO: Editorial Centro Investigaciones Sociológicas 619 p. (2004) ¿MÁS ALLÁ DE LA MODERNIDAD? LAS DIMENSIONES DE LA INFORMACIÓN, LA COMUNICACIÓN Y LAS NUEVAS TECNOLOGIAS

GÓMEZ ÁLVARO. 695 p. Coedición: Alfaomega-Rama; SEGURIDAD INFORMATICA Y LA PROTECCIÓN DE DATOS

DEL PESO NAVARRO EMILIO; PIATTINI VELTHUIS MARIO G., Editorial Ra-ma 708 páginas (12/2005) AUDITORIA INFORMÁTICA: UN ENFOQUE PRÁCTICO. 2 EDICIÓN AMPLIADA Y REVISADA

Sitios en la web

http://www.cybsec.com/ES/articulos/default.php 12/10/2005 Incidentes en seguridad informática. Lic. Julio C. Ardita Fecha de consulta 12/02/2022

http://www.cybercrime.gov/
El reporte del año 2002 del FBI y del Computer Security Institute acerca del
crimen por computadora. Fecha de consulta 12/03/2022

www.irchelp.org/irchelp/security/bo.html
Back Orifice
Anthony Stirk aka Upuaut
Fecha de consulta 12/03/2022

http://www.cybsec.com/ataque.pdf994 Incidentes de ataques a las empresas. Lic. Julio C. Ardita Fecha de consulta 12/03/2022

http://www.un.org/spanish/aroundworld/othersites.htm Clasificación de delitos informáticos elaborada por la ONU.
Organización de las Naciones Unidas
Fecha de consulta 12/03/2022

http://vil.nal.com/vi/default.aspx
Laboratorio McAfee con información detallada de virus, troyanos, agujeros y como infectan los sistemas.
McAfee
Fecha de consulta 12/03/2022

http://www.unisys.com.mx/press_room_mx/07052006.html La pequeña y mediana empresa en México y su adopción en tecnología informática
Unisys de Mexico.
Fecha de consulta 12/03/2022

http://ciberia ya.com/Mundoundergroun/nukers.htm

Desarrollo de Nukers
Fecha de consulta 12/03/2022

http://www.pandasecurity.com/spain/enterprise/solutions/
Proteja su organización con soluciones integradas
Panda Security
Fecha de consulta 12/03/2022

http://www.symantec.com/es/mx/home_homeoffice/index.jsp# Protección completa y automatizada para todo el contenido importante.
Symantec Corporation. Fecha de consulta 12/03/2022

http://usinfo.state.gov/journals/itps/1101/ijps/pj63fbi.htm
Proteger a las empresas Norteaméricanas del terrorismo cibernético.
Paul Rodgers (Jefe Ayudante, Unidad de Extensión y Apoyo de Campo Centro Nacional de Protección de Infraestructuras Oficina Federal de Investigaciones)

Fecha de consulta 12/03/2022

http://www.isaca.org.mx/CGI
BIN/isaca/mambo45 1/index.php?option=content&task Seguridad de la Información: Moda o Necesidad?
Edmundo Rodriguez Valenzuela (Director de Auditoria Especializada) Fecha de consulta 12/03/2022

http://www.isaca.org.mx/CGI
BIN/isaca/mambo451/index.php?option=content&task=view&id=51&ltemid=2
Seguridad de la Información: ¿Dejarla a la suerte?
Por Guadalupe Castañeda Campos CPA, CISA (Socia del área de Control y Administración de Riesgos Electrónicos (CARe) de Mancera Ernst & Young) Fecha de consulta 12/03/2022

http://www.isaca.org.mx/CGI
BIN/isaca/mambo451/index.php?option=content&task=view&id=5081temid=2
Auditoria de Seguridad
M. A. Zeuz Zamora Herrera (Auditor Adjunto) Fecha de consulta 14/03/2022

ANEXOS

Anexo Nº. 1.- Encuesta al personal de empleados y de servicios

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
ESCUELA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Instrumento: Encuesta. Empleados ( )
Tipo: Documental P. de Servicios ( )
Modalidad: Participativa
Objetivo: Establecer las estrategias de mejora en el sistema de Seguridad de la Información en la Corporación Nacional de Telecomunicaciones CNT EP, del Cantón Babahoyo, que permita incrementar la satisfacción al cliente y el rendimiento financiero de la institución.

De la manera más comedida le estamos solicitando su colaboración a fin de proceder a suministrar la presente información:

- Le anticipamos que la presente encuesta es de carácter reservada.
- Marque con una **X** la opción que estime conveniente.

No	PREGUNTA
1	**¿Cree usted que las instalaciones físicas de CNT EP son las adecuadas para desempeñar bien su labor?** A. Si ( ) B. No ( ) C. En Parte ( )
2	**¿Cómo califica usted los recursos materiales y suministros con los que cuenta para brindar el servicio al cliente?** A. Muy buenos ( ) B. Regulares ( ) C. Malos ( )
3	**¿Cuál considera usted que es la mejor estrategia para mejorar el servicio en la CNT EP?** A. Capacitar al empleado para brindar atención eficiente B. Agilizar los trámites de crédito C. Disminuir los tiempos de espera del cliente
4	**¿Cree usted que el tiempo que utiliza para la prestar un servicio en la CNT**

	EP es el adecuado? A. Si ( ) B. No ( ) C. A veces ( )
5	**¿Cuál considera usted que es la mayor causa de quejas en el servicio por parte de los clientes?** A. Falta de agilidad en la atención B. Tramites de crédito complicados C. Falta de capacitación del personal que atiende al cliente
6	**¿Considera usted que mediante un programa de capacitación en Seguridad de la Información, permitirá mejorar el servicio de la institución?** A. Si ( ) B. No ( ) C. En Parte ( )
7	**¿Considera usted que la remuneración que recibe por su labor es el adecuado respecto a la función que usted cumple?** A. Si ( ) B. No ( ) C. En Parte ( )
8	**¿Cada qué tiempo recibe usted capacitación en los sistemas de seguridad de la información, por parte del departamento de capacitación de la CNT EP?** A. Cada 6 meses B. Cada año C. Más de un año

Anexo Nº. 2.- Encuesta a clientes.

Instrumento: Encuesta. Clientes ( )
Tipo: Documental
Modalidad: Participativa
Objetivo: Establecer las estrategias de mejora en el sistema de Seguridad de la Información en la Corporación Nacional de Telecomunicaciones CNT EP, del Cantón Babahoyo, que permita incrementar la satisfacción al cliente y el rendimiento financiero de la institución.

De la manera más comedida le estamos solicitando su colaboración a fin de proceder a suministrar la presente información:

- Le anticipamos que la presente encuesta es de carácter reservada.
- Marque con una **X** la opción que estime conveniente.

No	PREGUNTA
1	**¿Al integrarse como cliente de la CNT EP se le facilito la información de manera rápida?** A. Si ( ) B. No ( ) C. En Parte ( )
2	**¿Cree usted la información que se da a los clientes al momento de buscar un servicio en la CNT EP es la adecuada?** A. Si ( ) B. No ( ) C. En Parte ( )
3	**¿Ha tenido algún inconveniente con el personal de atención al momento de solicitar algún servicio?** A. Si ( ) B. No ( ) C. A veces ( )

4	**¿Cómo considera usted que es la fluidez de los procesos para atender los requerimientos?** A. Rápido ( ) B. Lento ( ) C. Muy lento ( )
5	**¿Cree usted que el tiempo que utiliza para la prestación de un servicio es adecuado?** A. Si ( ) B. No ( ) C. En Parte ( )
6	**¿Qué calificación le da usted al servicio que recibe por parte del personal que lo atiende en la CNT EP?** A. Excelente ( ) B. Regular ( ) C. Mala ( )
7	**¿Cómo califica la actitud con la que el personal que atiende al cliente ofrece información de los servicios de la CNT EP**? A. Excelente ( ) B. Regular ( ) C. Mala ( )
	¿Cuál considera usted que es el aspecto que debe mejorar la institución para brindarle un mejor servicio? A. Capacitar al empleado para brindar atención eficiente B. Agilizar los trámites de los servicios solicitados C. Disminuir los tiempos de espera del cliente

Anexo Nº. 3.- Entrevista a las autoridades

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
ESCUELA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Instrumento: Entrevista. Empleados ( )
Tipo: Documental P. de Servicios ( )
Modalidad: Participativa
Objetivo: Establecer las estrategias de mejora en el sistema de Seguridad de la Información en la Corporación Nacional de Telecomunicaciones CNT EP, del Cantón Babahoyo, que permita incrementar la satisfacción al cliente y el rendimiento financiero de la institución.

De la manera más comedida le estamos solicitando su colaboración a fin de proceder a suministrar la presente información:

- Le anticipamos que la presente encuesta es de carácter reservada.
- Marque con una **X** la opción que estime conveniente.

No	PREGUNTA
1	**¿Cree usted que la CNT EP cumple con las metas administrativas que se propone?** A. Si ( ) B. No ( ) C. A veces ( )
2	**¿El personal que trabaja en la CNT EP es capacitado constantemente para dar un buen servicio al cliente?** A. Siempre ( ) B. regularmente ( ) C. Nunca ( )
3	**¿Considera usted que el departamento de capacitación de la CNT EP, ha cumplido con seminarios de actualización o talleres dedicados a mejorar la seguridad de la información?** A. Si ( ) B. No ( ) C. En parte ( )
4	**¿Considera usted que es necesario capacitar constantemente a los empleados para que den buen servicio a los clientes respetando la**

	política de seguridad de la información? A. Si ( ) B. No ( ) C. A veces ( )
5	**¿Considera usted que mediante un programa de capacitación en seguridad de la información, permitirá mejorar la imagen de la institución?** A. Si ( ) B. No ( ) C. En parte ( )
6	**¿Cuál considera que es la mayor debilidad en el ambiente interno de la CNT EP respecto al servicio ofrecido a los clientes?** A. Falta de capacitación del talento humano B. Escasa cultura organizacional C. Mucho tiempo de espera del cliente
7	**¿Cree usted que es necesario un buzón de sugerencias en la CNT EP?** A. Si ( ) B. No ( ) C. Tal vez ( )
8	**¿Por cuál de estos motivos cree usted que los colaboradores y clientes hacen más uso de los servicios de la CNT EP?** A. tecnología B. Costumbre C. economía.

Anexo Nº. 4.- Guía de Observación

Instrumento: **Guía de Observación**
Tipo: Documental
Modalidad: Participativa
Objetivo: Establecer las estrategias de mejora en el sistema de Seguridad de la Información en la Corporación Nacional de Telecomunicaciones CNT EP, del Cantón Babahoyo, que permita incrementar la satisfacción al cliente y el rendimiento financiero de la institución.

De la manera más comedida le estamos solicitando su colaboración a fin de proceder a suministrar la presente información:

- Le anticipamos que la información proporcionada es de carácter reservada.

CORPORACION NACIONAL DE TELECOMUNICACIONES CNT EP LOS RIOS.

1.- Nombre del Documento: Sistema de atención a clientes

Área de: Ventanilla.

2.- Contexto del documento: Es un listado en donde se anotan determinadas características generales que se cumplen dentro de la atención a clientes.

3.- Descripción del contenido del documento:

Actividades	SCP	SCA	SCI
La atención al cliente es de calidad.			
Ha sido capacitado servicio de atención a clientes			
Los mobiliarios con que cuenta son aceptables.			
La infraestructura del área de Ventanillas es ideal para la			

atención de los clientes.			
Cuenta con los insumos adecuados para la atención a los clientes.			
La atención a clientes es de esmero y dedicación personalizada.			
Coordina sus actividades con el resto de las áreas de la corporación.			

SCP = Se cumple plenamente; SCA = Se cumple aceptablemente; SCI = Se cumple insatisfactoriamente.

4.- Análisis del documento:

Comentarios:

Sugerencias:

Responsable de la Guía

Nombre del Investigador..... Fecha.....

Anexo Nº. 5.- Ficha de Contenidos.

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
ESCUELA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Instrumento: **Ficha de Contenidos.**
Tipo: Documental
Modalidad: Participativa
Objetivo: Establecer las estrategias de mejora en el sistema de Seguridad de la Información en la Corporación Nacional de Telecomunicaciones CNT EP, del Cantón Babahoyo, que permita incrementar la satisfacción al cliente y el rendimiento financiero de la institución.

De la manera más comedida le estamos solicitando su colaboración a fin de proceder a suministrar la presente información:

- Le anticipamos que la información proporcionada es de carácter reservada.

Departamento (___). **Área (___).**

1.- Nombre del Documento:

2.- Contexto del documento:

3.- Descripción del contenido del documento:

1.	
2.	
3.	
4.	
5.	

4. Análisis de los documentos:

Nombre del Investigador..... Fecha.....

Anexo Nº. 6.- Cuadro operativo

TEMA	PROBLEMA (s)	OBJETIVO (s)	HIPÓTESIS
Amenazas, vulnerabilidades y su incidencia en el sistema informático de la red Corporación Nacional de Telecomunicaciones CNT E.P Los Ríos	**GENERAL**	**GENERAL**	**GENERAL**
	¿Cómo implementar un adecuado sistema de detección de las amenazas y debilidades del sistema informático de la Corporación Nacional de Telecomunicaciones?	Potenciar el sistema de seguridad informática en la Corporación Nacional de Telecomunicaciones CNT EP Agencia Los Ríos para lograr mejorar la productividad de la empresa.	Potenciando el sistema de seguridad informática en la Corporación Nacional de Telecomunicaciones CNT EP Agencia Los Ríos, mejorará la productividad de la empresa
	DERIVADOS	ESPECIFICOS	PARTICULARES
	¿Cuenta actualmente con un sistema de detección de amenazas la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos?	Fundamentar de Bases Teóricas confiables, los sistemas de detección de amenazas y la seguridad informática.	Determinado un sistema de detección de amenazas la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos. Mejora su productividad.
	¿Por qué el sistema actual de detección de amenazas no cumple con las expectativas que los usuarios requieren afectando la calidad en la atención en la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos?	Identificar las necesidades y exigencias actuales de la CNT EP para diseñar adecuadamente estrategias de seguridad informática.	Identificada las necesidades y exigencia del sistema actual de detección de amenazas se optimizo el sistema y cumple con las expectativas que los usuarios requieren mejorando la calidad en la atención Corporación Nacional de Telecomunicaciones CNT EP Los Ríos.
	¿Cómo el sistema de detección de amenazas y debilidades de los sistemas informáticos afectan la calidad en la atención y no contribuyen al desarrollo y crecimiento de la organización en la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos?	Proponer estrategias adecuadas que permitan potenciar los sistemas de seguridad informática de CNT EP	Diseñado el plan de capacitación y de mejora continua sobre el sistema de detección de amenazas y debilidades de los sistemas informáticos de la Corporación Nacional de Telecomunicaciones CNT EP Los Ríos. Se perfecciono el perfil profesional del talento Humano

Anexo Nº. 7.- Operacionalización de las variables.

Variable Dependiente.

HIPÓTESIS	VARIABLES	DEFINICIONES CONCEPTUALES/ OPERACIONALES	DIMENSIONES	INDICADORES	ÍTEMS	INSTRUMENTOS
Potenciando el sistema de seguridad informática en la Corporación Nacional de Telecomunicaciones CNT EP Agencia Los Ríos, mejorará la productividad de la empresa.	**VD.** Seguridad de la información.	consiste en el resguardo de la información que se maneja por medios magnéticos, y en ella está incluida toda clase de archivos, ya sea personales, privados, organizacionales, financieros, políticos, ambientales, estadísticos, institucionales, entre otros.	Satisfacción Necesidades Posicionamiento Proceso Interacción social	Eficacia Efectividad Toma de decisiones. Responsabilidad de la gestión. Cumplimiento de estándares.		Encuesta Entrevista Guía de observación Ficha de contenidos.

Variable Independiente.

HIPÓTESIS	VARIABLES	DEFINICIONES CONCEPTUALES/ OPERACIONALES	DIMENSIONES	INDICADORES	ÍTEMS	INSTRUMENTOS
Potenciando el sistema de seguridad informática en la Corporación Nacional de Telecomunicaciones CNT EP Agencia Los Ríos, mejorará la productividad de la empresa.	**VI** Satisfacción del cliente	Es un término que hace referencia a la satisfacción que tiene un cliente con respecto a un producto que ha comprado o un servicio que ha recibido, cuándo éste ha cumplido o sobrepasado sus expectativas.	Necesidades Posicionamiento Proceso interno Interacción social Entrega de servicios.	Eficacia Efectividad Toma de decisiones. Responsabilidad de la gestión. Cumplimiento de estándares.		Encuesta Entrevista Guía de observación Ficha de contenidos.

Babahoyo, 7 de marzo del 2022

Licenciado
Eduardo Gáleas Guijarro, MAE
DECANO DE LA FACULTAD DE
ADMINISTRACION, FINANNZAS E INFORMÁTICA

Presente.-

De mi consideración:

Yo, ARACELLY CASTRO TRIVIÑO, con cargo de JEFE FINANCIERO Y SOPORTE LOS RIOS (e) de la CNT EP LOS RIOS autorizo a la señorita estudiante KARLA YLEANA SANCHEZ MELENDRES con cedula de identidad 1204741456, a proceder con la realización del proyecto cuyo tema es: "AMENAZAS, VULNERABILIDADES Y SU INCIDENCIA EN EL SISTEMA INFORMÁTICO DE LA RED DE CNT EP LOS RÍOS".

Particular que comunico a usted, para fines pertinentes.

Atentamente

Ing. Aracelly Castro Triviño.
JEFE FINANCIERO Y SOPORTE LOS RIOS (e)
CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP

UNIVERSIDAD TÉCNICA DE BABAHOYO

FECHA: 27/4/2022
HORA: 2:54

SR(A).
ING. MARIA ISABEL GONZALEZ VALERO
COORDINADOR DE LA UNIDAD DE TITULACIÓN DE LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA
EN SU DESPACHO.-

DE MI CONSIDERACIÓN:

EN ATENCIÓN A LA DESIGNACIÓN COMO DOCENTE TUTOR PARA GUIAR EL TRABAJO DE TITULACIÓN CON EL TEMA:

MODALIDAD	FASE	TEMA
PROYECTO DE INVESTIGACION	INFORME FINAL DE INVESTIGACIÓN	AMENAZAS Y VULNERABILIDADES Y SU INCIDENCIA EN EL SISTEMA INFORMáTICO DE LA RED DE LA CORPORACIóN NACIONAL DE TELECOMUNICACIONES LOS RIOS

PERTENECIENTE A EL/LOS ESTUDIANTES:

FACULTAD	CARRERA	ESTUDIANTE
FAFI	SISTEMAS DE INFORMACION (REDISEÑADA)	SANCHEZ MELENDRES KARLA YLEANA

AL RESPECTO TENGO A BIEN INFORMAR QUE EL/LOS ESTUDIANTES HAN CUMPLIDO CON LAS DISPOSICIONES ESTABLECIDAS EN EL REGLAMENTO E INSTRUCTIVO DE TITULACIÓN DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO, EN LOS TIEMPOS ESTABLECIDOS PARA EL EFECTO.

POR LO ANTERIORMENTE EXPUESTO, EL TRABAJO DE TITULACIÓN ES APROBADO POR QUIEN SUSCRIBE, AUTORIZANDO CONTINUAR CON EL PROCESO LEGAL PERTINENTE

POR LA ATENCIÓN QUE SE SIRVA DAR AL PRESENTE ME SUSCRIBO.

ATENTAMENTE,

UNIVERSIDAD TÉCNICA DE BABAHOYO

WELLINGTON ISAAC MAMZA CRUZ
DOCENTE TUTOR DEL EQUIPO DE TITULACIÓN

UNIVERSIDAD TÉCNICA DE BABAHOYO

Por Ti UTB

FECHA: 27/4/2022
HORA: 2:55

FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA
UNIDAD DE TITULACIÓN

SEGUIMIENTO DE PROYECTOS DE TITULACIÓN

DOCENTE TUTOR:	MALIZA CRUZ WELLINGTON ISAAC
ESTUDIANTES:	SANCHEZ MELENDRES KARLA YLEANA
PERIODO TITULACIÓN:	DICIEMBRE 2021 - ABRIL 2022
MODALIDAD DE TITULACIÓN:	PROYECTO DE INVESTIGACIÓN
FASE DE MODALIDAD:	INFORME FINAL DE INVESTIGACIÓN
PROYECTO DE TITULACIÓN:	AMENAZAS Y VULNERABILIDADES Y SU INCIDENCIA EN EL SISTEMA INFORMáTICO DE LA RED DE LA CORPORACIóN NACIONAL DE TELECOMUNICACIONES LOS RIOS

INFORMACIÓN DEL PROYECTO DE TITULACIÓN

AMENAZAS Y VULNERABILIDADES Y SU INCIDENCIA EN EL SISTEMA INFORMáTICO DE LA RED DE LA CORPORACIóN NACIONAL DE TELECOMUNICACIONES LOS RIOS					
FASE	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
INFORME FINAL DE INVESTIGACIÓN	2022-04-11	2022-04-28	TERMINADO	100%	HABILITADO

INFORMACIÓN DE ACTIVIDADES DEL PROYECTO

INTRODUCCIÓN					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
INTRODUCCION	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO I - IDEA O TEMA DE INVESTIGACIÓN					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
IDEA DE INVESTIGACIóN	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO I - MARCO CONTEXTUAL					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
MARCO CONTEXTUAL	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO I - SITUACION PROBLEMÁTICA					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
SITUACIóN PROBLEMáTICA	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO I - PLANTEAMIENTO DEL PROBLEMA					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
PLANTEAMIENTO DEL PROBLEMA	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO I - DELIMITACIÓN DE LA INVESTIGACIÓN					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
DELIMITACIóN DEL PROBLEMA	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO I - JUSTIFICACIÓN					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
JUSTIFICACIóN	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO I - OBJETIVO DE INVESTIGACIÓN					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO

OBJETIVOS	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO II - MARCO TEORICO					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
MARCO TEóRICO	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO II - HIPÓTESIS					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
HIPóTESIS	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO III - RESULTADOS OBTENIDOS DE LA INVESTIGACIÓN					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
RESULTADOS	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO III - CONCLUSIONES ESPECÍFICAS Y GENERALES					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
CONCLUSIONES	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO III - RECOMENDACIONES ESPECÍFICAS Y GENERALES					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
RECOMENDACIONES	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO IV - PROPUESTA DE APLICACIÓN DE RESULTADOS					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
PROPUESTA DE APLICACIóN	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO IV - RESULTADOS ESPERADOS DE LA ALTERNATIVA					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
RESULTADOS ESPERADOS	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO IV - BIBLIOGRAFÍA					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
BIBLIOGRAFíA	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

CAPÍTULO IV - ANEXOS					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
ANEXOS	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

TRABAJO FINAL					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
TRABAJO FINAL	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

RESUMEN Y PALABRAS CLAVE					
ACTIVIDAD	F. INICIO	F. FIN	PROCESO	PORC.	ESTADO
PALABRAS CLAVES	2022-04-19	2022-04-26	TERMINADO	100%	HABILITADO

SANCHEZ MELENDRES KARLA YLEANA
ESTUDIANTE

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN
FINANZAS E INFORMÁTICA

Curiginal

Document Information

Analyzed document	PROYECTO DE INVESTIGACIÓN - KARLA SÁNCHEZ MELENDRES. (URKUND).docx (D131747489)
Submitted	2022-03-28T05:35:00.0000000
Submitted by	
Submitter email	ksanchez456@fafi.utb.edu.ec
Similarity	6%
Analysis address	wmaliza.utb@analysis.urkund.com

Sources included in the report

W	URL: https://docplayer.es/207601083-Instituto-superior-tecnologico-bolivariano-de-tecnologia.html Fetched: 2022-03-28T05:35:26.1430000	1
W	URL: https://es.wikipedia.org/wiki/Corporaci%C3%B3n_Nacional_de_Telecomunicaciones Fetched: 2022-03-28T05:35:01.2900000	1
SA	**Amenazas y vulnerabilidades.pdf** Document Amenazas y vulnerabilidades.pdf (D129505273)	3
SA	**1483978968_215__java1.docx** Document 1483978968_215__java1.docx (D24839902)	1