UNIVERSIDAD NACIONAL DEL SANTA

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"PLAN DE SEGURIDAD INFORMÁTICO PARA MEJORAR LA CALIDAD EN EL SERVICIO DEL CALL CENTER DE LA EMPRESA TELSAT PERÚ SAC"

TESIS PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR:

Bach. ANGULO CASTILLO ALEXA MADELYN

ASESORA:

DRA. DIANA CECILIA MUÑOZ CASANOVA

CHIMBOTE - PERÚ

2014

UNIVERSIDAD NACIONAL DEL SANTA

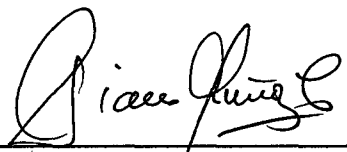
FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"PLAN DE SEGURIDAD INFORMÁTICO PARA MEJORAR LA CALIDAD EN EL SERVICIO DEL CALL CENTER DE LA EMPRESA TELSAT PERÚ SAC"

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

Revisado y aprobado por:



DRA. DIANA CECILIA MUÑOZ CASANOVA
ASESOR

"UNIVERSIDAD NACIONAL DEL SANTA"

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

)E SEGURIDAD INFORMÁTICO PARA MEJORAR LA DAD EN EL SERVICIO DEL CALL CENTER DE LA EMPRESA TELSAT PERU SAC"

INFORME DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

Sustentado y aprobado ante el siguiente jurado:

Dr. SIXTO DÍAZ TELLO	Ms. CARLOS GUERRA CORDERO
PRESIDENTE	SECRETARIO
Dra. DIANA MUÑOZ CASANOVA	Ing. PEDRO MANCO PULIDO
INTEGRANTE	ACCESITARIO

DEDICATORIA

A mi padre celestial, por darme la vida

y brindarme su amor cada día.

A mis padres Santos Angulo y Casilda Castillo, por su sacrificio, apoyo incondicional y ejemplo de trabajo y lucha ante las adversidades de la vida.

A mis hermanos Giovanna, Maribel, Aurea, David y Eder por su constante apoyo y por compartir conmigo muchos momentos.

AGRADECIMIENTO

A Dios nuestro Señor ya que sin su guía y protección no habría sido posible alcanzar una de mis metas trazadas en el largo camino de la superación.

A la Dra. Diana Cecilia Muñoz Casanova, asesora del presente informe, por su valioso aporte en el desarrollo de la presente tesis.

A todos los profesores de la Escuela de Ingeniería de Sistemas e Informática quienes con sus enseñanzas contribuyeron en mi formación profesional.

ÍNDICE

CAPÍTULO II: PLANTEAMIENTO DE LA INVESTIGACIÓN

CAPÍTULO III: MARCO TEÓRICO

CAPÍTULO IV: DESARROLLO DE LA METODOLOGÍA

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABLAS

RESUMEN

El presente trabajo tiene por objetivo proponer un Plan de Seguridad Informático basado en el **Estándar Internacional ISO/IEC 27002,** para mejorar la calidad en el Servicio del call center de la empresa Telsat Perú SAC.

El Estándar Internacional ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información en base a once secciones que involucran desde políticas de seguridad, controles de acceso, continuidad del negocio hasta cumplimiento legal.

Mediante el desarrollo del Plan de Seguridad Informático se ha podido establecer una cultura de la seguridad en la empresa. Asimismo se le ha permitido establecer a la empresa sus propios procedimientos de seguridad, los cuales deben estar enmarcados por las políticas que conforman este plan.

ABSTRACT

The present work have go as objective to propose a Computer Security Plan based on the International Standard ISO / IEC 27002 to improve the quality of call center service company Telsat Peru SAC.

The International Standard ISO / IEC 27002 provides best practice recommendations in the management of information security based on involving eleven sections from security policies, access controls, business continuity to legal compliance.

Through the development of Computer Security Plan has been able to establish a safety culture in the company. It also has allowed the company to establish its own security procedures, which must be framed by the policies that make up this plan.

PRESENTACIÓN

SEÑORES MIEMBROS DEL JURADO:

En cumplimiento a lo dispuesto en el Reglamento General de Grados y Títulos de la Facultad de Ingeniería de la Universidad Nacional de la Santa, de la Escuela Académico Profesional de Ingeniería de Sistemas e Informática, presento a vuestra consideración el presente informe de tesis titulado: **"PLAN DE SEGURIDAD INFORMÁTICO PARA MEJORAR LA CALIDAD EN EL SERVICIO DEL CALL CENTER DE LA EMPRESA TELSAT PERÚ SAC"** ; como requisito para optar el título profesional de Ingeniero de Sistemas e Informática.

El informe de tesis tiene como lugar de aplicación la Empresa Telsat Perú SAC cuyo propósito consiste en elaborar un Plan de Seguridad Informático con la finalidad de proteger la información y los activos de la organización, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos; para mejorar la calidad en el servicio del call center.

Espero que la presente tesis sirva de referencia y aporte para futuras investigaciones afines al tema en estudio.

Atentamente,

Bach. Angulo Castillo Alexa Madelyn

INTRODUCCIÓN

Cada día, la informática adquiere más relevancia en la vida de las personas y en las empresas. Actualmente ninguna empresa puede funcionar sin informática, a través de ella, todo se resuelve con mayor facilidad. El mundo está informatizado, lo que trae con ello muchos beneficios, pero también los hace vulnerables a los diferentes accidentes o daños si no se cuentan con un sistema de seguridad. Entre ellos, se pueden mencionar el robo, destrucción o modificación de información, fraude, etc.; ya sea por personas desde dentro o fuera de la empresa.

A fin de brindar la más completa protección empresarial, se requiere de un sistema de seguridad, por tanto es vital implementar un Plan de Seguridad Informático.

El propósito de establecer este Plan de Seguridad Informático para Telsat Perú SAC, es proteger la información y los activos de la empresa, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos; asimismo las responsabilidades que debe asumir cada uno de los trabajadores mientras permanezcan en la empresa. Estas políticas surgen como una herramienta para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de tal forma que permitan a la empresa cumplir con su misión.

El proponer e implantar esta política de seguridad requiere un alto compromiso de la empresa, agudeza técnica para establecer fallas y deficiencias, y constancia para renovar y actualizar dicha política en función de un ambiente dinámico.

Para la generación de las políticas mencionadas, resulta conveniente desarrollar un Plan de Seguridad Informático que evalúe el cumplimiento de los objetivos institucionales con respecto a la seguridad de la información y emitir recomendaciones que contribuyen a mejorar su nivel de cumplimiento.

existentes en lo relativo a controles de seguridad; Análisis de Riesgos; Formulación del Plan de Seguridad Informático.

En el Capítulo V, en éste capítulo se realiza la contrastación de la hipótesis propuesta en la presente investigación.

Finalmente se anotan las conclusiones y recomendaciones de esta investigación y la bibliografía utilizada para su desarrollo.

CAPÍTULO I

LA EMPRESA

1.1 Naturaleza

1.1.1 Nombre o Razón Social

TELSAT PERÚ SAC.

1.1.2 Domicilio legal

Av. Enrique Meiggs N° 2200, Chimbote

1.1.3 Logo de la Empresa

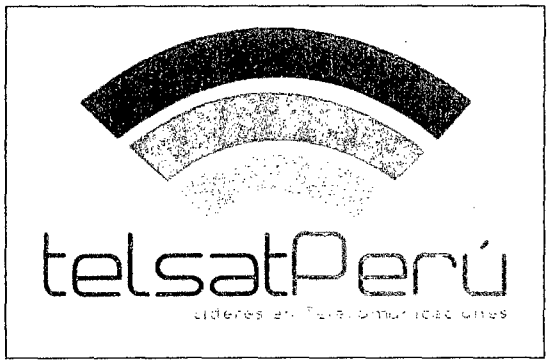


Figura N° 01: Logo de la empresa Telsat Perú SAC

1.1.4 Objetivos

1.1.4.1 Objetivo General

Ser una parte importante e innovadora del proceso de soluciones tecnológicas, servicios de redes y telecomunicaciones, principalmente basados en la tecnología VoIP que exceda las expectativas de nuestros clientes, atendiendo agresivamente el gran crecimiento y las altas posibilidades del mercado basándonos en la integridad, el trabajo en equipo y la urgencia.

1.1.4.2 Objetivos Específicos

- Ofrecer satisfacción al cliente a través de la calidad de productos y servicios.
- Aplicar políticas de mejora continua para la realización de sus procesos, dando más relevancia al uso de tecnología.

1.2 Descripción de la Empresa

TELSAT PERÚ SAC es una empresa privada que ha desarrollado una amplia gama de soluciones diseñadas para empresas de distintos rubros y características, ofreciendo diversos servicios como:

- Venta e instalación de equipos para enlaces inalámbricos.
- Instalación de Internet Inalámbrico Residencial de Banda Ancha.
- Instalación de Sistema de Televigilancia por internet.
- Venta de línea telefónica a través de su call center, el cual presta servicio para terceros en Estados Unidos (Latinos en EE.UU).

1.3 Misión

"Somos una empresa que brinda el servicio de venta de equipos de cómputo, instalación de internet inalámbrico residencial de banda ancha, instalación de sistemas de televigilancia por internet y servicio de call center. Orientada a satisfacer las necesidades y aspiraciones de nuestros clientes. Somos un aporte positivo para la sociedad, generando empleo directo e indirecto dentro de un buen ambiente de trabajo, pagando impuestos y obteniendo un justo margen de utilidad".

1.4 Visión

Ser una empresa líder de alto conocimiento técnico que ofrece soluciones innovadoras y eficientes, brindando la mejor atención en el servicio; con un equipo humano profesional capacitado, creativo, permanentemente motivado y comprometido con la creación de valor para la empresa y la comunidad.

1.5 Estructura Orgánica:

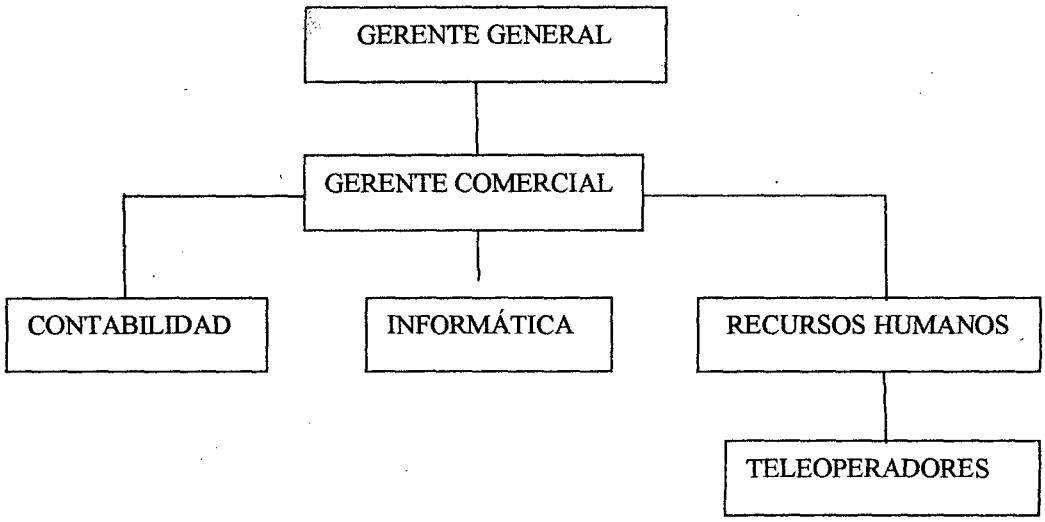


Figura N° 02: Organigrama de la empresa

1.6 POLÍTICAS

POLÍTICAS DE CALIDAD

- "Nosotros nos esforzaremos para la excelencia en todo lo que hagamos. Fijaremos nuestras metas para ser reconocidas por nuestros clientes como un líder en calidad total y satisfacción del cliente. Nosotros

proporcionaremos soluciones innovadoras y los productos de calidad más altos y servicios en base a un costo competitivo."

- La Calidad es definida como "satisfacer las expectativas del cliente el 100% del tiempo".

POLÍTICAS CON LOS CLIENTES

- Ofrecer productos que satisfagan sus requerimientos cumpliendo con los estándares de calidad y requisitos legales asociados.

POLÍTICAS CON SUS TRABAJADORES

- Desarrollar y promover el bienestar y la capacitación constante de los trabajadores.
- Mantener y mejorar las condiciones de higiene y seguridad en el ambiente de trabajo.
- Involucrar a sus trabajadores con el cumplimiento de los planes de la empresa.

POLÍTICAS CON EL ENTORNO SOCIAL

- Promover el desarrollo socio económico de la comunidad.

POLÍTICAS CON EL MEDIO AMBIENTE

- Cuidar el medio ambiente y procurar su mejoramiento previniendo la contaminación, utilizando eficientemente los recursos y cumpliendo con la legislación y reglamentaciones ambientales aplicables a nuestras actividades.

POLÍTICAS CON LOS PROVEEDORES

- Evaluar permanentemente la capacidad de los proveedores para suministrar productos y servicios que cumplan con nuestras exigencias de calidad.

CAPÍTULO II

PLANTEAMIENTO DE LA INVESTIGACIÓN

2.1 EL PROBLEMA

2.1.1. REALIDAD PROBLEMÁTICA

Telsat Perú SAC es una empresa que brinda el servicio de venta y configuración de equipos para enlaces inalámbricos, instalación de Internet inalámbrico residencial de banda ancha e instalación de Sistemas de Televigilancia por internet. Asimismo cuenta con un call center, el cual trabaja para empresas extranjeras como Nuera Telecom y Banco Santander ofreciendo su servicio de llamadas telefónicas internacionales y venta de tarjetas de débito respectivamente, esto para estar a la vanguardia de la tecnología y en su afán de brindar un servicio de comunicación de información eficiente y de forma transparente para el personal.

Telsat Perú SAC tiene 9 años en el mercado y cuenta en la actualidad con 30 pc´s las cuales funcionan en su totalidad para el call center, el cual utiliza software como: Eyebeam, Spark, Software de Oficina, Antivirus Corporativo y Sistemas Operativos no licenciados, para ello cuenta con los respectivos servidores que dan soporte a las diferentes aplicaciones y servicios.

En el año 2009, año en que se inicia el funcionamiento del call center, su promedio en ventas mensuales era de 150 ventas aproximadamente,

teniendo 14 teleoperadores (ventas hechas para la Empresa Nuera Telecom).

En la actualidad, con el mismo número de teleoperadores, su promedio mensual es de 100 ventas aproximadamente, notándose claramente una disminución de los ingresos mensuales de la empresa.

El motivo principal en estos índices es la deserción de los empleados por la insatisfacción del funcionamiento de la red informática lo cual implica: fallas en la transmisión de los datos en la red, pérdida en la fluidez de la comunicación con los clientes, lentitud, saturación e inoperatividad en la red además ante un corte de fluido eléctrico se cortan las conversaciones de una manera intempestiva y al no contar con los equipos necesarios para evitarlo se pierde la comunicación con el cliente y éste muchas veces ya no contesta cuando se le vuelve a llamar disminuyendo la posibilidad de captar un cliente mas.

En cuanto al cableado se puede observar que está expuesto a interferencias como corriente eléctrica ya que no se encuentran protegidos en su totalidad por canaletas y éstas a su vez están deterioradas. Además la red no cuenta con controles de seguridad que protejan la integridad, confidencialidad y disponibilidad de los datos que en ella se transmiten, por lo tanto la empresa tiene una red informática que no cumple las normas o estándares internacionales de seguridad haciendo que esté vulnerable a ataques, intromisiones de personas no autorizadas, desastres naturales, desastres

informáticos, etc. lo que ha ocasionado la pérdida de clientes y recursos para la empresa.

Telsat Perú SAC con la finalidad de mejorar el servicio que brinda en su call center está dispuesta a seguir un plan de seguridad Informático.

2.1.2. FORMULACIÓN DEL PROBLEMA.

¿De qué manera el plan de seguridad informático mejorará la calidad en el servicio del call center de la empresa Telsat Perú SAC?

2.2 JUSTIFICACIÓN

El plan de seguridad informático permitirá:

➢ **Justificación Tecnológica:**

- Proteger la información y los activos de la organización, asegurando la confidencialidad, integridad y disponibilidad de los datos.
- Mejorar el servicio que brinda el call center de la empresa Telsat Perú SAC mediante el plan de seguridad informático.
- Controlar los diferentes accesos a los sistemas que maneja la empresa.

➢ **Justificación Económica:**

Aumentar los ingresos económicos considerablemente, ya que cuanto más estable y eficiente se encuentre la red informática del call center, mayor será la calidad en el servicio y la posibilidad de captar más clientes.

➢ **Justificación Social:**

* Incrementar el nivel de concienciación del personal, sobre la importancia y sensibilidad de la información y servicios críticos; para que permitan cumplir con la misión de la empresa.

* El presente proyecto también trata de dar una guía a las empresas sobre como dar solución a los problemas de Seguridad Informática que presenten y de la importancia de ésta para evitar cualquier problema de seguridad informática en el futuro.

➢ **Justificación Ambiental:**

El plan de seguridad informático permitirá asegurar el cumplimiento de normas ambientales dentro del call center que permitan contribuir al cuidado del medio ambiente.

2.3 OBJETIVOS

2.3.1. Objetivo General

Proponer un plan de seguridad informático para mejorar la calidad en el servicio del call center de la empresa Telsat Perú SAC.

2.3.2. Objetivos Específicos

- Realizar una revisión bibliográfica a cerca de Planes de Seguridad Informáticos.

- Recopilar y organizar la información necesaria para entender a la empresa.

- Analizar el estado del software, los equipos informáticos y de telecomunicaciones del centro de cómputo de la empresa Telsat Perú SAC.

- Analizar los controles de seguridad informáticos en la empresa Telsat Perú SAC de acuerdo a la Norma ISO/IEC 27002.

- Desarrollar un análisis de riesgos en la empresa Telsat Perú SAC. , con el propósito de determinar cuáles de los activos de la empresa tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos.

- Definir las políticas de seguridad que conforman el Plan de Seguridad Informático, basados en el estándar de seguridad internacional ISO/IEC 27002, que garantice minimizar los riesgos identificados.

- Elaborar el Plan de Seguridad Informático para la empresa Telsat Perú SAC.

2.4 HIPÓTESIS.

El plan de Seguridad Informático mejora la calidad en el servicio del call center de la empresa Telsat Perú SAC.

2.5 VARIABLES

- Variable Independiente

  Plan de seguridad informático.

Indicadores:

Número de controles de Seguridad aplicados.

- ❖ Variable Dependiente

Mejorar la calidad en el servicio del call center

Indicadores:

- Número de ventas por mes del teleoperador
- Número de llamadas perdidas por falla en la red
- Número de quejas por falla en la red del teleoperador

2.6 POBLACIÓN

Todos los procesos informáticos que se realizan en la empresa Telsat Perú SAC.

2.7 MUESTRA

Tomaremos como muestra los procesos del call center de la empresa Telsat Perú SAC, porque son los procesos que requieren un mayor nivel de seguridad.

2.8. DISEÑO DE LA INVESTIGACIÓN

Grupo Único con medición previa y posterior.

G1 O1 X O2

Donde:

O1 : Medición inicial de indicadores, antes de la aplicación de la variable independiente.

X : Variable Independiente, Plan de Seguridad Informático.

O2 : Medición final de indicadores, después de la aplicación de la variable independiente.

2.9. METODOLOGÍA

- Etapa I : Análisis del Sistema de Seguridad informático actual
- Etapa II : Análisis de las once (11) secciones referidas a la seguridad informática.
- Etapa III : Desarrollo del análisis de riesgos
- Etapa IV : Formulación del plan de seguridad informático

CAPÍTULO III

MARCO TEÓRICO

3.1 CALL CENTER

También llamados "centros de llamadas", se trata de una oficina donde un grupo de personas específicamente entrenadas se encarga de brindar algún tipo de atención o servicio telefónico, lo cual está determinado por cada empresa.

Los trabajadores de un call center pueden realizar llamadas (para tratar de vender un producto o un servicio, realizar una encuesta, etc.) o recibirlas (para responder las inquietudes de los clientes, tomar pedidos, registrar reclamos). En algunos casos, el call center se especializa en una de las dos tareas (realizar o recibir los llamados) mientras que, en otros, cumplen con ambas funciones.

Es importante destacar que el call center puede ser operado por la propia compañía o tercerizado en una empresa externa. Hay firmas que se dedican a establecer centros de llamadas (con la infraestructura necesaria y el personal entrenado) y comercializan dicha prestación.

El call center cuenta con estaciones de trabajo que incluyen computadoras, teléfonos, auriculares con micrófonos (headsets) conectados a interruptores telefónicos y una o más estaciones de trabajo pertenecientes a los supervisores del sector.

Una de las ventajas que ofrece un call center a una empresa es que centraliza la atención. Si no se cuenta con un call center, todas las llamadas llegarían a distintas oficinas y resultará más complicado canalizarlas y registrarlas. El call center, en cambio, tiene como única función facilitar la comunicación.

Los operarios están capacitados para resolver los asuntos por su propia cuenta y recién derivan la llamada a un ejecutivo en casos excepcionales.
El Call Center, hoy en día constituye un recurso estratégico para las empresas, debido a que numerosas personas utilizan los teléfonos para realizar consultas, pedir información o hacer negocios con lo que se ahorran tiempo, esfuerzo y dinero.

Actualmente este servicio está siendo implementado en la mayoría de las empresas de grandes volúmenes de producción ya que sus relaciones comerciales diarias exceden la capacidad humana para ser controladas por una sola telefonista.

Figura N° 03: Call center

3.2 TELEOPERADOR

Es una persona que trabaja desde un ordenador, sentado delante de uno de ellos del que recibe y en el que introduce información, con un auricular y un micrófono a través de los cuales gestiona llamadas telefónicas para captar nuevos clientes, absolver consultas, etc.

3.3 RED INFORMÁTICA

Llamada también red de computadoras o red de ordenadores, es un conjunto de equipos informáticos conectados entre sí por medio de distintos elementos de conexión, tales como:

- Cables.
- Tarjetas de red.
- Dispositivos inalámbricos, etc.

La finalidad de una Red Informática es compartir información, recursos (software: programas y datos; hardware: impresoras, escáneres, etc.). Además nos permite asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el coste general de estas acciones. Un ejemplo es Internet, la cual es una gran red de millones de computadoras ubicadas es distintos puntos del planeta interconectadas básicamente para compartir información y recursos.

La red informática puede a su vez dividirse en diversas categorías, según su alcance (red de área local o LAN, red de área metropolitana o MAN, red de área amplia o WAN, etc.), su método de conexión (por cable coaxial, fibra óptica, radio, microondas, infrarrojos) o su relación funcional (cliente-servidor, persona a persona), entre otras.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este último, estructura cada red en siete (7) capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a cuatro (4) capas.

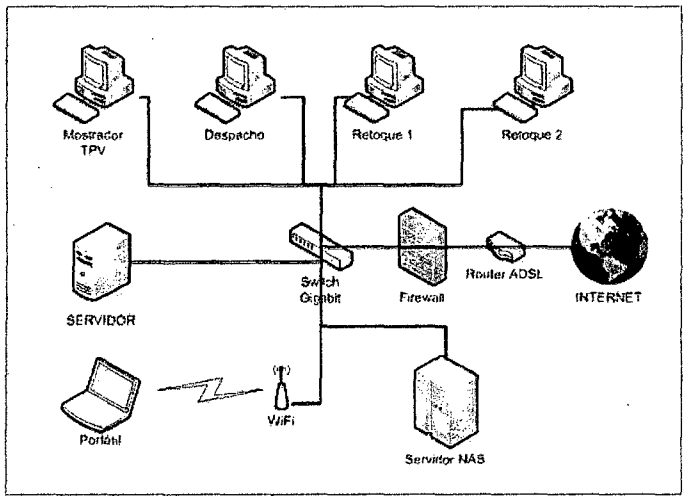


Figura N° 04: Red Informática

3.4 ACTIVO INFORMÁTICO

Bienes de una organización, que se encuentran relacionados directa o indirectamente con la actividad informática, entre ellos se cuentan:

A) La información mecanizada (no están incluidos los documentos fuentes que la generan).

B) Medios de comunicación que se utilizan para la transmisión de datos mecanizados (redes de computadoras, correo electrónico, etc.).

C) Medios magnéticos y ópticos de almacenamiento de la información (cinta, cartuchos, diskettes, discos, etc.)

D) Programas y aplicaciones de la Institución, ya sea desarrollados por ésta, adquiridos o alquilados a terceros.

E) Manuales, procedimientos y reglamentaciones afines al área de informática (Plan de Contingencia, procedimientos de seguridad, etc.).

3.5 INFORMACIÓN

En sentido general, la información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Los datos sensoriales una vez percibidos y procesados constituyen una información que cambia el estado de conocimiento, eso permite a los individuos o sistemas que poseen dicho estado nuevo de conocimiento tomar decisiones pertinentes acordes a dicho conocimiento.

Desde el punto de vista de la ciencia de la computación, la información es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno. En principio la información, a diferencia de los datos o las percepciones sensibles, tienen estructura útil que modificará las sucesivas interacciones del ente que posee dicha información con su entorno. También constituye cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuída y almacenada.

3.6 SEGURIDAD INFORMÁTICA

3.6.1 DEFINICIÓN

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y por tanto requiere una protección adecuada. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio,

minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La información adopta diversas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La primera medida para gestionar en forma adecuada la seguridad de la información, es definir una Política de Seguridad de la Información, es decir, una declaración formal de las pautas que deben ser respetadas para el manejo de la información, cualquiera sea su representación y ubicación. La gestión de la información, la cual implica administrar, redactar las políticas, normas y procedimientos, implementarlas y verificar su cumplimiento, debe constituir un área estratégica del Organismo.

3.6.2 VULNERABILIDAD DE LOS SISTEMAS INFORMÁTICOS

Los tres elementos principales a proteger en cualquier sistema informático son: el software, el hardware y los datos.

- **Hardware**: Conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, diskettes...) o tarjetas de red.
- **Software**: Conjunto de programas lógicos que hacen funcionar al *hardware*, tanto sistemas operativos como aplicaciones.

- **Datos**: Conjunto de información lógica que manejan el *software* y el *hardware*, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos.

Además, generalmente se habla de un cuarto elemento llamado **fungible**; que son los aquellos que se gastan o desgastan con el uso continuo, como papel de impresora, tóneres, cintas magnéticas, diskettes.

3.6.3 MEDIDAS BÁSICAS PARA LA SEGURIDAD INFORMÁTICA

1) Antivirus: Un antivirus es un programa informático específicamente diseñado para detectar y eliminar virus, programado para revisar la PC de forma periódica.

2) Cortafuegos: Un cortafuegos o "firewall" es un 'software' destinado a garantizar la seguridad en las comunicaciones vía Internet al bloquear las entradas sin autorización a su ordenador y restringir la salida de información.

3) Actualizar frecuentemente sus aplicaciones con los "parches de seguridad": Las vulnerabilidades que se detectan en los programas informáticos más utilizados (navegadores de Internet, procesadores de texto, programas de correo, etc.) precisan de un 'software' que las compañías fabricantes ponen a disposición de sus clientes en actualizaciones, llamadas "parches de seguridad", vía Internet.

4) Software Legal: Los programas originales garantizan el correcto funcionamiento ofreciendo una mayor seguridad y fiabilidad; además

aumenta la calidad de soluciones, servicios y su desarrollo tecnológico, se disminuyen las posibilidades de entrada de virus en los sistemas, se incrementa la rentabilidad y la competitividad de la empresa, se dispone de los servicios de asistencia técnica y de mantenimiento ofrecidos por los fabricantes, etc.

Se recomienda adquirir el software a través de distribuidores autorizados.

5) Precaución con el correo electrónico: Conviene analizar, antes de abrir, todos los correos electrónicos recibidos y sospeche de los mensajes no esperados, incluso si provienen de algún conocido.

6) Prudencia con los archivos: Se recomienda no descargar de Internet ni de adjuntos de correos electrónicos, ni distribuya o abra ficheros ejecutables, documentos, etc, no solicitados.

7) Copias de Seguridad: Es importante realizar de forma periódica copias de seguridad de la información más valiosa.

8) Ayudar a los demás: No es bueno distribuir indiscriminadamente bromas de virus, alarmas, o cartas en cadena. No se debe contestar a los mensajes 'spam' (publicidad no deseada) ya que al hacerlo se reconfirma la dirección.

9) Mantenerse Informado: Sobre todo de las novedades de seguridad informática, a través de los boletines de las compañías fabricantes de 'software', así como de los servicios de información y boletines del Centro de Alerta Antivirus, sobre las nuevas apariciones de virus informáticos.

10) Utilizar la papelera: Todos aquellos correos que resulten sospechosos, si no se conoce al remitente o presentan un 'Asunto' desconocido, deben ir a la papelera. Es importante vaciarla después.

3.7 PLAN DE SEGURIDAD INFORMÁTICO

Es la expresión gráfica del Sistema de Seguridad Informático diseñado y constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una entidad y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

Por tanto, el Plan de Seguridad Informático es un documento en el que establecen las políticas, y acciones que permiten garantizar la prestación de servicios y asegurar la información contenida en un sistema computacional, considerando los lineamientos para promover la planeación, el diseño y la implementación de un modelo de seguridad en la Empresa, con el fin de establecer una cultura de la seguridad en la organización.

El propósito de establecer éste plan es proteger la información y los activos de la organización, tratando de preservar:

a) Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información.

b) su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.

c) su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

3.8 STANDAR INTERNACIONAL ISO/IEC 27002

3.8.1 ISO

ISO es el acrónimo de International Organization for Standardization. Aunque si se observan las iniciales para el acrónimo, el nombre debería ser IOS, los fundadores decidieron que fuera ISO, derivado del griego "*isos*", que significa "igual". Por lo tanto, en cualquier país o en cualquier idioma, el nombre de la institución es ISO, y no cambia de acuerdo a la traducción de "International Organization for Standardization" que corresponda a cada idioma. Se trata de la organización desarrolladora y publicadora de Estándares Internacionales más grande en el mundo. ISO es una red de instituciones de estándares nacionales de 157 países, donde hay un miembro por país, con una Secretaría Central en Geneva, Suiza, que es la que coordina el sistema.

ISO es una organización no gubernamental que forma un puente entre los sectores públicos y privados.

Respecto al origen de la organización ISO, oficialmente comenzó sus operaciones el 23 de febrero de 1947 en Geneva, Suiza. Nació con el objetivo de "facilitar la coordinación internacional y la unificación de los estándares industriales."

3.8.2 IEC

IEC es el acrónimo de International Electrotechnical Commission. Esta es una organización sin fines de lucro y también no gubernamental. Se ocupa de preparar y publicar estándares internacionales para todas las tecnologías eléctricas o relacionadas a la electrónica.

IEC nace en 1906 en London, Reino Unido, y desde entonces ha estado proporcionando estándares globales a las industrias electrotécnicas mundiales. Aunque como se acaba de decir, IEC nació en el Reino Unido, en el año de 1948 movieron su sede a Geneva, Suiza, ciudad en la que también se encuentra la sede de ISO.

3.8.3 ISO/IEC JTC1

ISO e IEC han establecido un comité técnico conjunto denominado ISO/IEC JTC1 (ISO/IEC Joint Technical Committee). Este comité trata con todos los asuntos de tecnología de la información. La mayoría del trabajo de ISO/IEC JTC1 es hecho por subcomités que tratan con un campo o área en particular. Específicamente el subcomité SC 27 es el que se encarga de las técnicas de seguridad de las tecnologías de información. Dicho subcomité ha venido desarrollando una familia de Estándares Internacionales para el Sistema Gestión y Seguridad de la Información. La familia incluye Estándares Internacionales sobre requerimientos, gestión de riesgos, métrica y medición, y el lineamiento de implementación del sistema de gestión de seguridad de la información. Esta familia adoptó el esquema de numeración utilizando las series del número 27000 en secuencia, por lo que a partir de

julio de 2007, las nuevas ediciones del ISO/IEC 17799 se encuentran bajo el esquema de numeración con el nombre ISO/IEC 27002.

3.8.4 ISO/IEC 27002

Anteriormente llamada ISO 17799, es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000 y con el título de Information technology - Security techniques - Code of practice for information security management. Tras un periodo de revisión y actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799 tiene su origen en Archivo: La norma británica British Standard BS 7799-1 que fue publicada por primera vez en 1995.

En España existe la publicación nacional UNE-ISO/IEC 17799 que fue elaborada por el comité técnico AEN/CTN 71 y titulada *Código de buenas prácticas para la Gestión de la Seguridad de la Información* que es una copia idéntica y traducida del Inglés de la Norma Internacional ISO/IEC 17799:2000. La edición en español equivalente a la revisión ISO/IEC 17799:2005 se estima que esté disponible en la segunda mitad del año 2006.

En Perú la ISO/IEC 17799:2000 es de uso obligatorio en todas las instituciones públicas desde agosto del 2004, cuando el Ing. César Vilchez propuso la norma al entonces Jefe de la ONGEI - PCM, Rafael Parra Erkel, quién aprobó la iniciativa, estandarizando de esta forma los diversos

proyectos y metodologías en este campo, respondiendo a la necesidad de seguridad por el uso intensivo de Internet y redes de datos institucionales, la supervisión de su cumplimiento esta a cargo de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI (www.ongei.gob.pe).

ISO/IEC 27002 es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. La seguridad de la Información se define en el estándar como: "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran). "

La versión de 2005 del estándar incluye las siguientes once secciones principales:

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad de la información

CAPÍTULO IV

DESARROLLO DE LA METODOLOGÍA

4.1 ANÁLISIS DEL SISTEMA DE SEGURIDAD INFORMÁTICO ACTUAL

4.1.1 ANÁLISIS DE LOS EQUIPOS INFORMÁTICOS

Telsat Perú SAC Asimismo cuenta con un sistema de red con las siguientes características:

- Tecnología : 10 Base T
- Velocidad : 10 / 100 Mbps
- Topología : Estrella
- Cable : UTP Categoría 5 E
- Switch : D – Link
- Sistema Operativo : Windows Server 2000 (Servidores) y Window Xp (Estaciones)
- Protocolo de comunicación : TCP/IP

➢ **HARDWARE**

o **Estaciones de Trabajo**

La empresa cuenta con las siguientes estaciones de trabajo:

N°	Marca	Procesador	HD	RAM	S.O	Cantidad
01	Compatible	Pentium III 800 Mhz	36 GB	256 MB	Windows XP	30

- Gestión de continuidad de negocio
- Conformidad

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre las once secciones aunque cada organización debe considerar previamente cuantos serán realmente los aplicables y según sus propias necesidades.

02	IBM	Pentium IV 2.8 GHz	100 GB	512 MB	Windows XP	03

Tabla N° 01: Hardware de las Estaciones de Trabajo

- **Servidores**

  La empresa cuenta con tres (03) servidores los cuales se detallan a continuación:

N	FUNCION	MARCA Y MODELO	PROCESADOR	HD	RAM	S.O
1	Red y Web	Compaq	Pentium IV 550 Mhz	4 SCSI 9 GB	64 MB	Windows server 2000
2	Base de Datos y Aplicaciones	Compatible	Pentium IV 800 Mhz	360 GB	256 MB	Windows server 2000
3	Archivos	IBM	Pentium IV 2.8 GHz	100 GB	512 MB	Windows Server 2000

Tabla N° 02: Hardware de los Servidores

- **Impresoras:**

  En el caso de las impresoras se tienen los siguientes equipos:

N°	Marca	Modelo	Tecnología de impresión	Usuario
1	HP	1560	TINTA	GERENTE COMERCIAL
2	HP LASERJET	P1110W	LASER	INFORMÁTICA

Tabla N° 03: Hardware de las Impresoras

- **Equipos de comunicación :**

N°	Dispositivo	Marca	N° Puertos	Cantidad
01	SWITCH CORE	D – Link	48	01
02	ROUTER	D – Link	04	01

Tabla N° 04: Hardware de los Equipos de comunicación

- **Equipos de Seguridad:**

  La empresa no cuenta con equipos de seguridad o contingencia ante una caída del fluido eléctrico u robos (UPS, grupo electrógeno, sensores, etc).

➢ **SOFTWARE**

- **Configuración:**

Todas las computadoras tienen asignadas la siguiente configuración:

- Sistema Operativo Microsoft Windows XP (Estaciones de trabajo)
- Sistema Operativo Microsoft Windows Server 2000 (Servidores)
- Ofimática: Microsoft Office 2010.
- Eyebeam
- Spark Messenger
- Win Zip versión 7.0

- **Aplicaciones**

  La empresa no cuenta con sistemas informáticos, todo el control lo realiza en hojas de cálculo de Excel. (Inventario de Equipos, Reporte de ventas semanales, mensuales, etc).

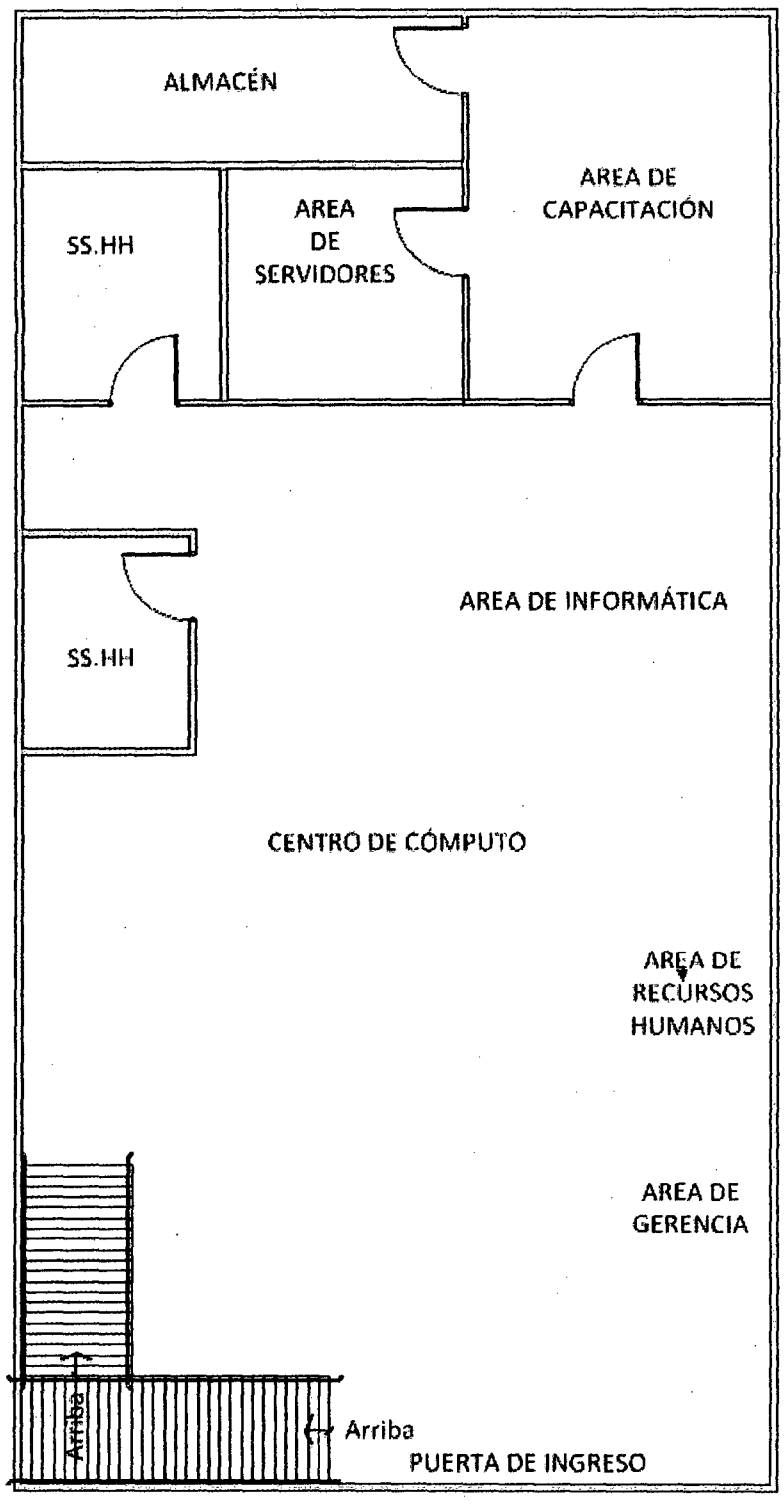


Figura N° 05: Diagrama Físico del Call Center de la empresa Telsat Perú SAC

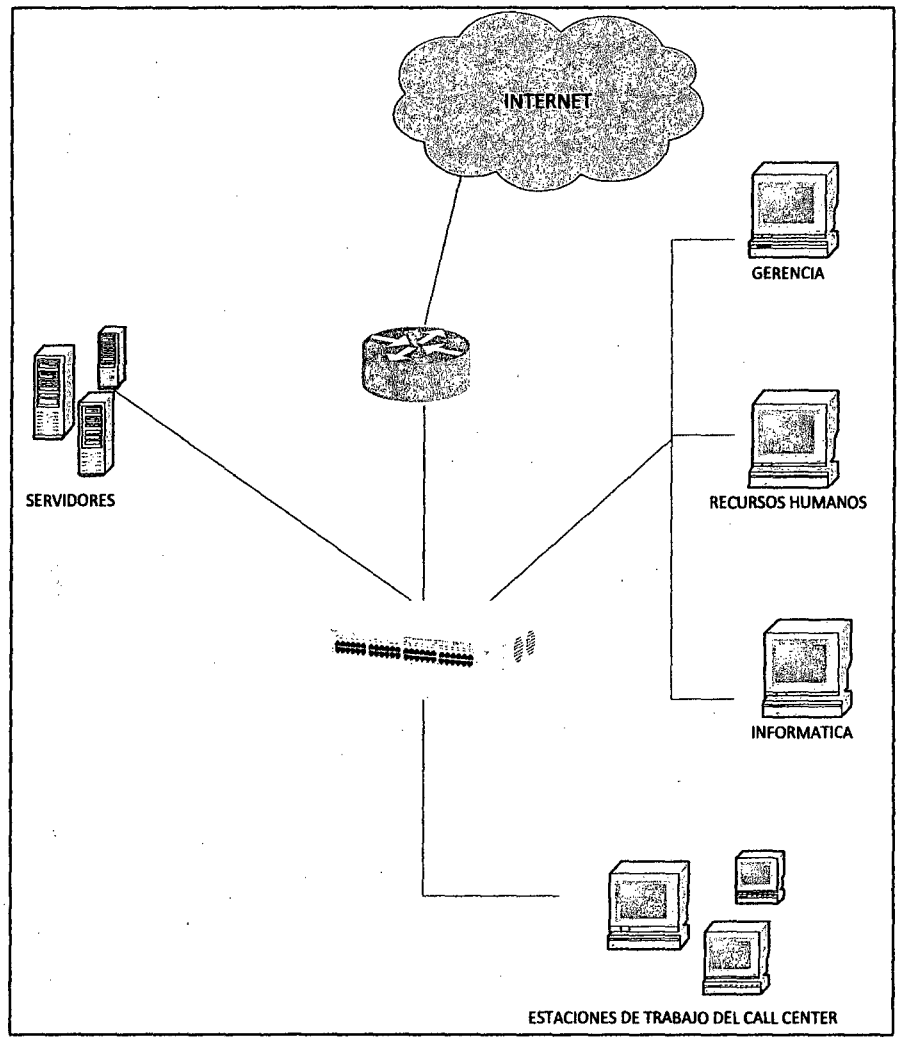


Figura N° 06: Diagrama Lógico de la red Informática de la Empresa Telsat Perú SAC

4.2 ANÁLISIS DE LAS ONCE (11) SECCIONES REFERIDAS A LA SEGURIDAD INFORMÁTICA

Para hacer un diagnóstico de la empresa en cuanto a Seguridad informática se ha tomado como ayuda la realización del cuestionario de diagnóstico basado en la norma ISO/IEC 27002.

4.2.1 EVALUACIÓN DE LA POLÍTICA DE SEGURIDAD (Anexo N° 1)

Problema N° 1:

La Empresa no cuenta con Políticas de Seguridad de la Información para proteger la información de posibles pérdidas en la confidencialidad, integridad y disponibilidad de los datos de la empresa. La información se encuentra vulnerable a los diferentes delitos y accidentes tales como: el robo, destrucción o modificación de información, fraude, cortes de fluído eléctrico intempestivo, etc.

Recomendación:

Elaborar y documentar la Política de Seguridad de la Información, cuya finalidad debe ser proteger y mantener la disponibilidad de la información de la empresa.

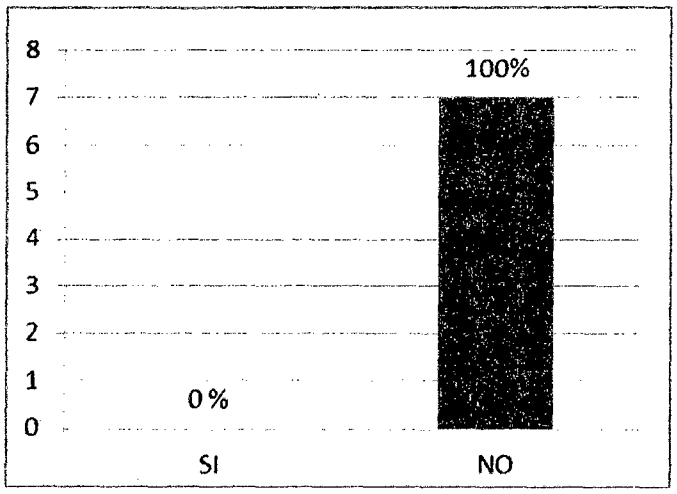


Gráfico N° 01: Evaluación de encuesta de Anexo N°1
Elaboración: Propia

4.2.2 EVALUACIÓN DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (Anexo N°2)

Problema N° 1:

La empresa no cuenta con un comité informático que permita coordinar y debatir los asuntos relacionados a ella, como promover el uso de nuevas tecnologías; adquirir nuevos equipos informáticos, implementar sistemas de información, etc., es decir velar por el desarrollo informático en la empresa. Sólo cuenta con un personal encargado del centro de cómputo que a su vez es el que ejecuta funciones de soporte y mantenimiento de los equipos.

Recomendación:

Se debe establecer la conformación de un comité informático para velar por el desarrollo informático de la empresa; que se encargue del manejo de datos, organización, planificación de políticas de seguridad, respaldo de datos, recuperación de datos a la hora de desastres, asimismo promover el uso de nuevas tecnologías; adquirir nuevos equipos informáticos, implementar sistemas de información etc. Dicho comité deberá también estar integrado por un usuario el cual determinará los requerimientos de la información.

Problema N° 2

No existe un Plan Operativo Informático sobre las actividades que se van a desarrollar (relacionadas con computadoras, aplicativos, proyectos, redes

Recomendación:

Se deberá asignar a una persona que conforma el comité informático para que se encargue de la administración de seguridad de la información, y ponga de conocimiento de ello a todo el personal de la empresa, además deberá controlar la protección de los activos informáticos de la empresa tanto físicos (instalaciones, hardware) como lógicos (software, datos).

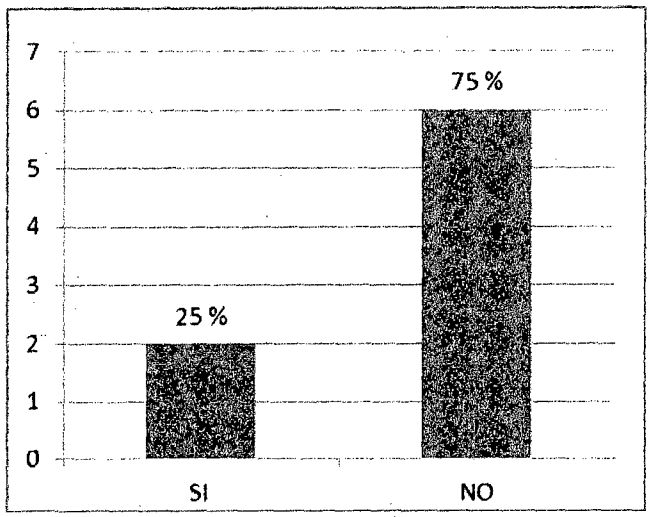


Gráfico N° 02: Evaluación de encuesta de Anexo N°2

Elaboración: Propia

4.2.3 EVALUACIÓN DE LA GESTIÓN DE ACTIVOS (Anexo N° 3)

Problema N° 1:

No se cuenta con un inventario de los activos de la empresa, solo se tiene una lista en hoja de cálculo, la relación del hardware que posee la empresa, el cual no recibe una inmediata actualización, no permitiendo garantizar una protección eficaz de los recursos.

Recomendación:

Telsat Perú SAC deberá realizar un inventario periódico de los activos de datos, software, equipos y servicios asociados a la tecnología de la información de esta manera saber qué hardware y software se tiene en cada computadora. Asimismo un inventario actualizado constantemente ayudará a administrar y realizar un seguimiento de las compras, versiones, números de serie y licencias del software; las fechas de garantía, de instalación, actualización o de eliminación.

Problema N° 2:

Los activos de información de la empresa no se clasifican formalmente según su importancia, lo que provocaría la mala asignación de controles de acceso, y así posibilitar la divulgación de la información.

Recomendación:

Sería conveniente que los activos de información se clasifiquen de acuerdo a su importancia teniendo en cuenta la confidencialidad y la disponibilidad que debe tener.

La clasificación de los activos de información de acuerdo a su importancia permite protegerla frente a pérdidas, divulgación no autorizada o cualquier otra forma de uso indebido; y asignar distintos niveles de controles de seguridad según la confidencialidad que sea necesaria.

Se podrían definir cuatro niveles de información: restringida, confidencial, uso interno y general.

Restringida: Información con mayor grado de sensibilidad; el acceso a ésta información debe ser autorizado.

Confidencial: Información sensible que sólo debe ser divulgada a aquellas personas que la necesiten para el cumplimiento de sus funciones.

Uso Interno: Datos generados para facilitar las operaciones diarias; deben ser manejados de una manera discreta, pero no requiere de medidas elaboradas de seguridad.

General: Información que es generada específicamente para su divulgación a la población general de usuarios.

Esta clasificación debe ser documentada e informada a todo el personal de la empresa la cual deberá evaluarse y actualizarse periódicamente.

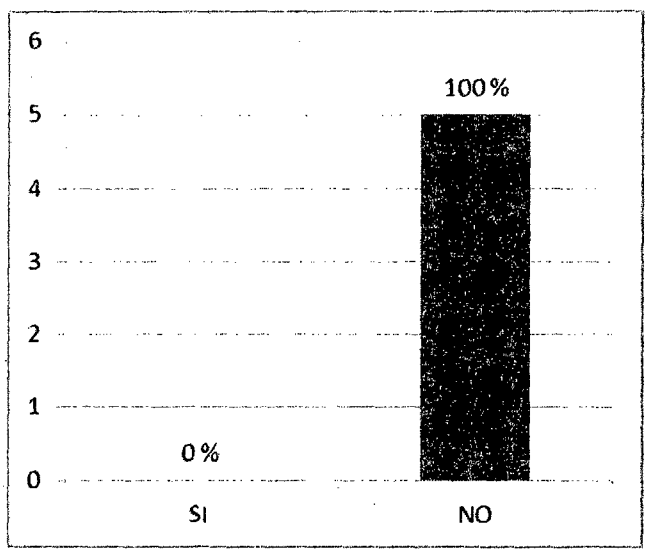


Gráfico N°03: Evaluación de encuesta de Anexo N°3

Elaboración: Propia

4.2.4 EVALUACIÓN DE LA SEGURIDAD LIGADA A LOS RECURSOS HUMANOS (Anexo N° 4)

Problema N° 1:

No existe un procedimiento exclusivo para el reclutamiento y selección del personal de la empresa, trayendo como consecuencia una posible falta en la confidencialidad, integridad o disponibilidad de parte de los empleados con la empresa.

Recomendación:

Se recomienda la elaboración e implementación de un procedimiento de reclutamiento que tenga en cuenta los siguientes aspectos relativos a la seguridad:

a)Definición del puesto: Para cada nueva vacante se debe definir la criticidad del puesto a cubrir según su responsabilidad y la información que maneja.

b)Selección: En la selección del personal se tendrá presente que deberán tener conocimiento básicos de informática (Microsoft office nivel usuario).

c)Contrato: El contrato laboral debe incluir los correspondientes acuerdos de confidencialidad, propiedad intelectual y protección de datos.

d)Comienzo: Durante los primeros días de trabajo, es recomendable que el trabajador asista a unas sesiones de formación donde se le introduzca en la normativa interna y de seguridad de la empresa, reciba el manual de normativa interna y firme el compromiso de cumplimiento del mismo.

e)Accesos: Se le debe informar a los trabajadores que el acceso a cierta información solo puede ser solicitado al responsable del área de informática.

Problema N° 2:

No se les pide certificado policial, judicial o penal, del personal a contratar, de esta manera se desconocen sus antecedentes y no se sabría que tipo de personal se contrata.

Recomendación:

La empresa deberá solicitar el correspondiente certificado penal, policial o judicial antes de contratar al personal.

Problema N° 3:

No se le brinda capacitación a los trabajadores, respecto a temas de seguridad de la información; y al no contar también con políticas de seguridad de la información no permite que el usuario comprenda sobre el buen uso del sistema y que esté dispuesto a cumplirlas.

Recomendación:

Es responsabilidad del área de informática promover, mediante un programa de concientización, la importancia de la seguridad de la información en todos los trabajadores del call center.

Problema N° 4:

No existe en la empresa un procedimiento de respuesta ante incidentes de seguridad. El principal problema de ésta situación consiste en que cuando existen errores o fallas , la presencia de algún virus, el usuario comunica verbalmente al encargado del centro de cómputo, quien asiste y soluciona su problema pero no registra estos errores o fallas que ocurren en el procesamiento de la información o en la red informática.

Recomendación:

Sería conveniente que se registren todos los errores y fallas que ocurren en el procesamiento de información o en los sistemas de comunicaciones a fin de tener un control de fallas.

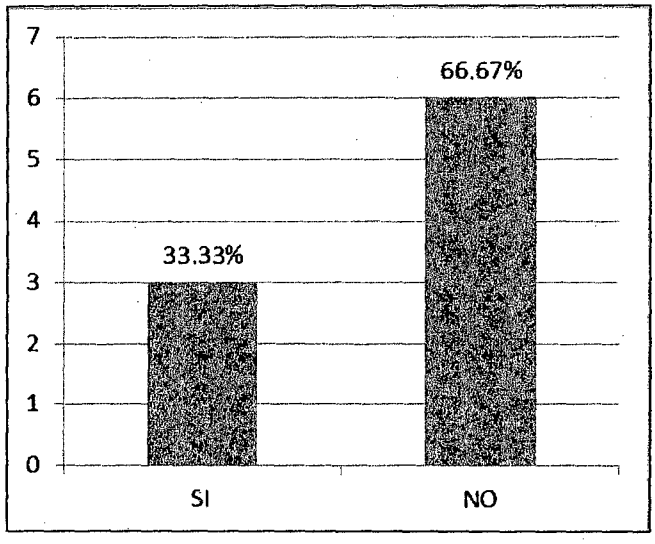


Gráfico N° 04: Evaluación de encuesta de Anexo N°4

Elaboración: Propia

4.2.5 EVALUACIÓN DE LA SEGURIDAD FÍSICA Y AMBIENTAL (Anexo N° 5)

La empresa y su centro de cómputo se encuentran ubicados en el segundo piso del bien inmueble. La construcción es de material noble, incluyendo el techo, iluminado eléctricamente, tiene ventilación natural y ambiente amplio.

Problema N° 1:

No existe un perímetro físico que divida a las áreas dentro de la empresa, sólo la habitación donde se encuentran los servidores, la cual tiene una dimensión de 4x3 m. Es el mismo lugar en donde funciona también el almacén y la vulnerabilidad de acceso está expuesta ya que siempre está con la puerta abierta. Asimismo dentro del mismo recinto existe un punto de agua potable.

Recomendación:

Se debería dividir físicamente las áreas dentro de la empresa, asimismo la habitación donde se encuentren los servidores deben ser exclusivamente para ellos, los cuales estarán bajo llave y cuyo acceso sólo estará permitido para el administrador u personal de informática. Los servidores nunca deberán ubicarse cerca de ductos de ventilación o junto al aire acondicionado. Elementos tales como motores y microondas pueden ocasionar interferencia con tracción eléctrica. También deberá evitarse la interferencia electromagnética (EMI). Sólo deberán utilizarse circuitos a tierra aislados.

El área en torno al servidor deberá mantenerse libre de desechos, desorden y sin ninguna tubería de agua en la habitación.

Problema N° 2:

Las computadoras de la empresa tienen los puertos USB deshabilitados. Sin embargo las computadoras en el call center poseen lectoras de CD habilitados y no hay ningún control sobre ellos lo que hace correr el riesgo de bootear desde este dispositivo y consecuentemente infectarse con algún virus.

Recomendación:

Sería conveniente que las lectoras de discos se deshabilitaran desde el BIOS de cada máquina. Si llega a ser necesario, para realizar alguna tarea de mantenimiento, el administrador de red puede ingresar al BIOS del equipo (utilizando la contraseña que él suministró), habilitar el dispositivo necesario y, una vez utilizado, deshabilitarlo nuevamente.

Problema N° 3:

No hay control de acceso a la configuración del BIOS de las computadoras y de los servidores. De ésta forma al momento del encendido de la máquina cualquiera podría modificar las opciones de configuración de los equipos.

Recomendación:

Sería conveniente que las máquinas tuvieran configurado un password de administrador en el acceso al setup (BIOS), para evitar que se modifiquen las configuraciones base de los equipos, esto podría aplicarse tanto a las computadoras como a los servidores. Estas contraseñas deberían gestionarlas el administrador de red, en todos los equipos de la red.

Problema N°4:

No se mantiene un registro de las personas que ingresan al área de informática o de empresa en general, lo que podría causar que personas desconocidas tengan acceso a la información de la empresa.

Recomendación:

Se debería tener un registro de todas las personas que ingresen a la empresa, en especial al área de informática.

Problema N°5:

No existe un Plan de mantenimiento preventivo ni correctivo que garantice el funcionamiento de los equipos de cómputo y de seguridad de la empresa; esta ausencia provocaría un retraso en las actividades, inoperatividad, acumulación de fallas y errores que afectan el rendimiento del personal y el logro de objetivos.

Recomendación:

Se sugiere realizar un plan de mantenimiento preventivo, consistente en limpieza, detección y corrección de fallas de hardware y software de:

Servidores, CPU´s, Monitores, impresoras y demás dispositivos; este programa permitirá minimizar el riesgo de presentarse un mantenimiento correctivo, evitando que su costo sea demasiado alto. Asimismo se deberá llevar un registro de control de los dispositivos que se instalan o remplazan en las computadoras.

Problema N° 6:

Ni el área donde se encuentran los servidores ni en el mismo call center se cuenta con un sistema de aire acondicionado, sobretodo en la época de verano , lo cual puede provocar un sobrecalentamiento de los equipos de cómputo y poner en riesgo los componentes internos de los mismos (tarjetas) por acumulación de calor.

Recomendación:

La empresa debe contar con un sistema de aire acondicionado, tanto para el call center como para la habitación donde se encuentran los servidores; de esta manera asegurar que el mismo permanezca por debajo de la temperatura operativa máxima.

Problema N° 7:

Cuando los empleados están en conversación directa con el cliente y se va la energía eléctrica se corta intempestivamente la conversación y se pierde la posibilidad de tener un cliente mas del servicio que se ofrece.

Recomendación:

La empresa debe contar con UPS automático, autonomía mínima de 15 minutos mínimo. Adicionalmente al UPS debe existir un Grupo Electrógeno a ser utilizado en casos de emergencia también, el cual debe ser probado periódicamente a fin de asegurar su operación.

Problema N° 8:

No existen planos descriptivos, permitiendo que no se determine la ubicación exacta e identificación de los puntos de red y recorrido del cableado, dificultando el mantenimiento del cableado en caso de ocurrir fallas del mismo.

Recomendación:

Se sugiere realizar un levantamiento de los planos descriptivos debidamente documentados, que permitan determinar la ubicación exacta e identificación de los puntos de red y recorrido del cableado, para un mantenimiento eficiente del cableado en caso de ocurrir fallas del mismo.

Problema N° 9:

La empresa no cuenta con personal de vigilancia las 24 horas, ni sensores de movimiento o cámaras de video vigilancia, lo cual la hace más vulnerable a posibles robos, saqueos, atracos, etc.

Recomendación:

Se recomienda a la empresa contratar personal de seguridad las 24 horas a fin de resguardar los activos de la empresa; asimismo deberá contar con sensores de movimiento y cámaras de video vigilancia que ayuden a detectar algo fuera de lo normal del movimiento de la empresa.

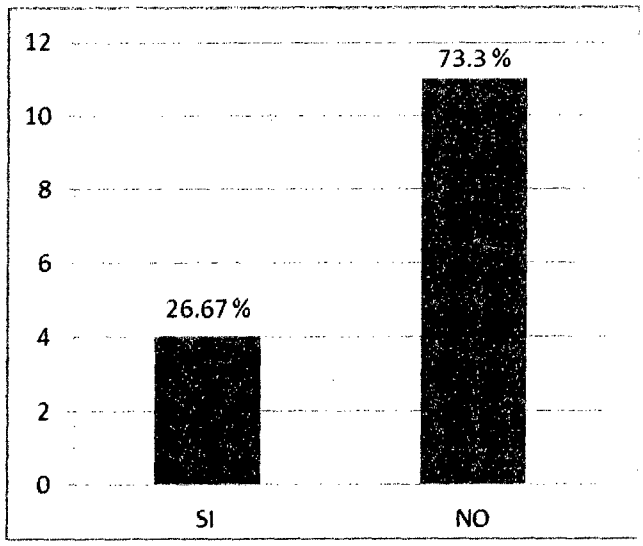


Gráfico N° 05: Evaluación de encuesta de Anexo N°5

Elaboración: Propia

4.2.6 EVALUACIÓN DE LA SEGURIDAD EN LA GESTIÓN DE COMUNICACIONES Y OPERACIONES (Anexo N° 6)

Problema N° 1:

La empresa no cuenta con documentación de los procedimientos y responsabilidades operacionales lo que traería como consecuencia el uso inadecuado de los recursos de la red y del desarrollo de las operaciones de la misma.

Recomendación:

Se debería contar con procedimientos de operación de los sistemas debiendo ser documentados y los cambios realizados a dichos procedimientos deben ser autorizados por la gerencia respectiva.

El contenido de la documentación de las operaciones de red deberá ser sencillo, claro y completo, de modo que pueda ser fácilmente comprendido por los usuarios.

Todas las tareas programadas en los sistemas para su realización periódica, deben ser documentadas.

Este documento debe incluir tiempo de inicio, tiempo de duración de la tarea, procedimiento en caso de falla, entre otros.

Problema N° 2:

La empresa no dispone de las licencias de antivirus para los equipos existentes; tiene instalados el NOD Antivirus versión 10.0, en las pcs de la estaciones de trabajo y administrativas, pero sin licencia.

Recomendación:

La empresa debe contar con un antivirus original, el cual debe actualizarse constantemente. Se sugiere desarrollar un procedimiento para la instalación de software antivirus en los servidores de la red y en todas las computadoras de la empresa.

Problema N° 3:

En caso de infección de virus no hay procedimientos formales a seguir. Lo que puede ocurrir que el virus no sea eliminado completamente del equipo y contagie a través de la red a los demás equipos, además de la posibilidad de pérdida de datos en los equipos infectados.

Recomendación:

Debería haber un procedimiento documentado a seguir para el caso que se encuentre un virus en el sistema. Se sugiere las siguientes actividades:

- Chequear el disco con el escaneo de virus para determinar si hay un virus, y qué virus es. Eliminar el virus.
- Cerrar los programas, apagar la máquina y bootear la computadora desde el disco de rescate del antivirus.
- Hacer un nuevo chequeo de virus en el disco duro.
- Chequear el resto de los dispositivos de datos (usb, etc.), para saber de donde vino el virus.
- Tratar de determinar la fuente del virus. La persona que hizo llegar el virus debe ser informada.
- Avisar a todos los usuarios del sistema que hayan intercambiado datos con la computadora infectada.

También es necesario brindar información a los usuarios, de las consecuencias que trae consigo la infección de virus en la red.

Problema N° 4:

No se cuentan con licencias para todo el software instalado en las diversas computadoras de la empresa, la cual constituye una amenaza, en caso de intervención de INDECOPI quien se encarga de administrar las licencias, provocaría un impacto en la imagen de la empresa y posibles cargos contra los directivos de la empresa.

Recomendación:

La empresa debe obtener cada software con su respectiva licencia y asi evitar un delito informático el cual se encuentra comprendido en el Art. 207, inciso A, del Código Penal.

Problema N° 5:

La empresa no cuenta con ningún procedimiento formal para la recuperación de los backups de los datos almacenados en los servidores y en los Cds. Las copias de respaldo son el principal método de recuperación de datos del que dispone la empresa y la ausencia de procedimientos para su implementación puede generar errores en el momento de un incidente. Sólo se realizan copias de seguridad de la base de datos en cd´s y en los discos duros de servidores los cuales no se guardan fuera de la empresa, lo cual podría originar la pérdida total de la información en caso de robo, incendio, etc.

Recomendación:

El área de sistemas deberá asignar un responsable que se encargue de realizar las copias de seguridad de los sistemas de aplicación, archivos de datos, base de datos e información, utilizando como medio de almacenamiento Cintas tape backup, siendo conveniente su encriptación, definiendo la periodicidad para efectuar los resguardos; y así estar prevenidos en caso de presentarse alguna contingencia.

Además se deberá adquirir con el tiempo nuevos servidores con última tecnología.

Se considera necesario que exista un procedimiento escrito y formal de política de backup.

Problema N° 6:

No existe un plano del cableado de la red informática lo que no permite la ubicación exacta e identificación de los puntos de red y recorrido del cableado, dificultando su mantenimiento en caso de ocurrir alguna falla.

Recomendación:

La empresa debe contar con los respectivos planos que describan la red informática de la empresa, los cuales deberán estar debidamente documentados y permitirán ubicar e identificar con exactitud los puntos de red y recorrido del cableado, en caso de falla o para su respectivo mantenimiento.

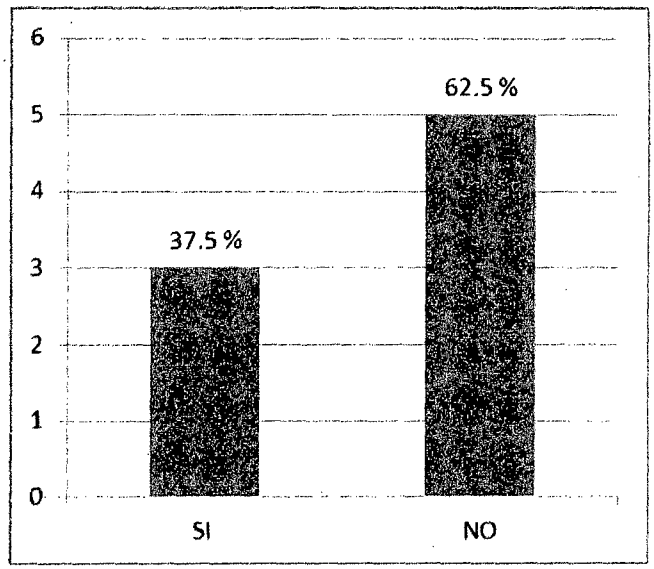


Gráfico N° 06: Evaluación de encuesta de Anexo N°6

Elaboración: Propia

4.2.7 EVALUACIÓN DEL CONTROL DE ACCESOS (Anexo 7)

Problema N° 1:

Para inicializar el S.O se pide al usuario que se ingrese el nombre del usuario y contraseña de acceso a la red. La empresa trabaja con el S.O Windows 2000 Server y como éste nos brinda la facilidad de administrar a los usuarios, por Grupos, permite mejorar los accesos y permisos para cada uno de los sistemas y de sus respectivos módulos. Por ejemplo tenemos el Grupo: Teleoperadores Nuera Telecom, Teleoperadores Santander; sin embargo los usuarios del sistema no tienen asignado una fecha de expiración del password, de manera que el usuario no es obligado, en ningún momento, a modificar su clave de acceso, siendo los mismos desde su fecha de creación, de manera que se facilita su revelación o robo.

Recomendación:

Se sugiere a los usuarios de la red cambiar su contraseña dentro de un periodo que no exceda los dos meses.

Problema N° 2:

Se detectó que cuando un usuario trata de ingresar al sistema e ingresa mal su contraseña n veces, el sistema no lo bloquea, es decir que puede seguir intentando ingresar la clave cuantas veces quiera, haciendo vulnerable el sistema.

Recomendación:

El sistema resultaría más eficiente si se considera que el número de intentos fallidos se restringiera a tres, permitiendo el bloqueo de usuarios al excederse de la cantidad mencionada anteriormente.

Problema N° 3:

La empresa no tiene ninguna restricción horaria al momento de permitir a un usuario el logeo al sistema. Lo cual podría pasar que un usuario no autorizado intente ingresar al sistema fuera del horario de trabajo, lo cual sería grave.

Recomendación:

Debería restringirse el horario en que puede ser utilizado el sistema informático de la empresa, de manera que:

-Las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan (debido a que diferentes grupos pueden tener diferentes horarios).

-Durante las vacaciones, días feriados o licencias las cuentas de usuarios deben desactivarse.

Problema N° 4 :

Los passwords no tienen una longitud mínima requerida por el sistema, solo tienen que respetar un largo máximo de 8 caracteres alfanuméricos. Al no haber una longitud mínima, los usuarios pueden poner un password de un solo carácter (por ejemplo un espacio, o un solo número) lo que las hace fácilmente descifrables, generando vulnerabilidades importantes en los datos que éstas protegen.

Recomendación:

Es necesario que exista un número mínimo de caracteres (8) que conforman el password. Además debe requerirse que dicha contraseña está compuesta de datos alfanuméricos, numéricos y caracteres especiales.

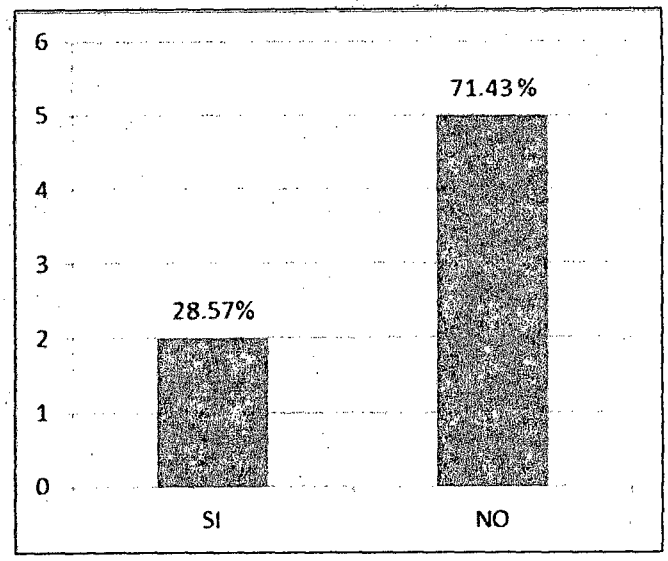


Gráfico N° 07: Evaluación de encuesta de Anexo N°7

Elaboración: Propia

4.2.8 EVALUACIÓN DE LA SEGURIDAD DE LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS INFORMÁTICOS (Anexo N° 8)

Problema N° 1:

Actualmente la empresa no cuenta con las licencias del Sistema Operativo de Redes : Windows Server 2000 y del sistema operativo XP y de Ofimática: Microsoft Office 2010 para la totalidad de equipos existentes de la empresa, tampoco se tiene actualizado los sistemas operativos; al no contar con las licencias constituye una amenaza, en caso de intervención de INDECOPI quien se encarga de administrar las licencias, provocaría posibles cargos contra la empresa.

Recomendación:

Realizar de manera inmediata la compra del software original para todos los equipos existentes y las licencias respectivas, de no hacerlo se estaría incurriendo en falta grave (delito informático), según el Art. 207, inciso A, del Código Penal.

Problema N° 2:

No hay aplicaciones desarrolladas en la empresa

Recomendación:

La empresa debería desarrollar sistemas informáticos como de almacén o inventario, de ventas, etc

Problema N° 3:

La empresa no cuenta con personal de desarrollo de sistemas y a la vez no existe un plan de desarrollo de sistemas formal durante el ciclo de vida del software. Lo que conlleva a un atrazo en cuanto a avance tecnológico para la empresa.

Recomendación:

Sería conveniente contar con personal desarrollador de sistemas informáticos que siga un plan de desarrollo, donde se definan la asignación de recursos, establecimiento de prioridades, administración de tiempos,

con el objeto de garantizar eficientemente el cumplimiento de las tareas propuestas.

Problema N° 4:

No existe documentación de los sistemas ya que no hay sistemas informáticos, todo el control se lleva mediante hojas de cálculo en Excel.

Recomendación:

Todo sistema informático implementado ha elaborarse debe ser documentado; asimismo se deben establecer normas y procedimientos para los desarrollos y su actualización.

Se sugieren los siguientes documentos para lograr una empresa eficiente: Objetivos, alcances, diagramas general y de funciones o de procesos, Diagrama Entidad Relación, diagrama de flujo, archivos de entrada-salida, responsable del módulo (analista que lo desarrolló), registro de modificaciones, lenguaje de programación, problemas o limitaciones conocidas, áreas de la organización a los que afecta, descripción del "hardware" y "software" utilizados, características de seguridad.

Es necesario que cada vez que se produzca una modificación en algún módulo del sistema, se modifique toda la documentación correspondiente.

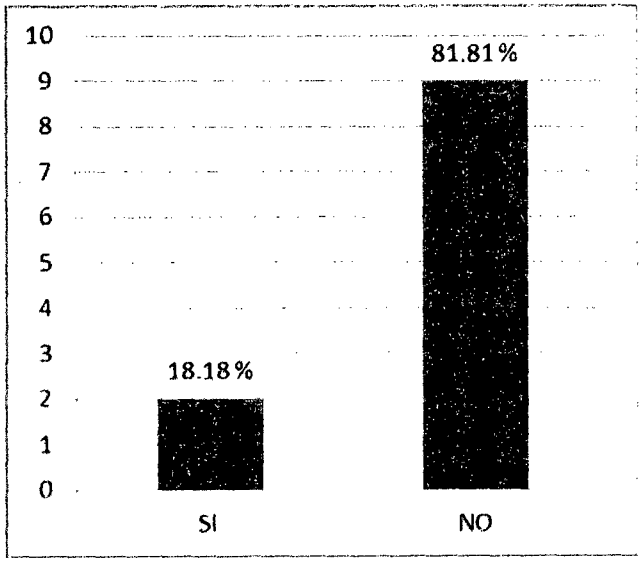


Gráfico N° 08: Evaluación de encuesta de Anexo N°8

Elaboración: Propia

4.2.9 EVALUACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ANEXO N° 09)

Pese a todas las medidas de seguridad pueden ocurrir incidentes en la seguridad. Por tanto, es necesario que el Plan de Contingencias incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

Un Plan de Contingencia de Seguridad Informática consiste en los pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en

parte, la capacidad funcional del sistema aunque, y por lo general, constan de reemplazos de dichos sistemas.

Se dice que el Plan de Contingencias es el encargado de sostener el modelo de Seguridad Informática planteado y de levantarlo cuando se vea afectado.

La recuperación de la información se basa en el uso de una política de copias de seguridad (Backup) adecuada.

Problema N° 1:

La empresa no cuenta con un Plan de Contingencias y de Recuperación que indique los procedimientos y acciones a seguir en caso de un eventual siniestro o desastre como: incendios, posibles fallas eléctricas, robos, inundaciones, sismos, etc.

Al no contar con éste Plan dificultaría las tareas de recuperación de la información en caso de posibles interrupciones en el procesamiento, impidiendo que la información sistematizada esté disponible para el desarrollo normal de las actividades y la toma de decisiones.

Recomendación:

La empresa deberá generar y documentar un Plan de Contingencias que incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles. Asimismo se le deberá realizar pruebas,

mantenimiento y evaluación constante a fin de asegurar la continuidad de las operaciones informáticas.

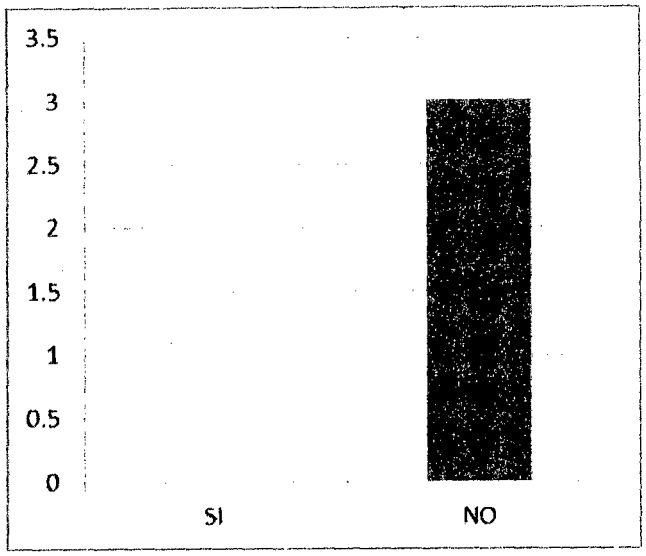


Gráfico N° 09: Evaluación de encuesta de Anexo N°9

Elaboración: Propia

4.2.10 EVALUACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (ANEXO N° 10)

Problema N° 1:

La empresa no cuenta con planes de continuidad y los servicios de recuperación de desastres que aseguren la viabilidad de la empresa protegiendo sus procesos críticos contra desastres y fallas mayores en los sistemas de información, así como de sus efectos y asegurando su establecimiento oportuno.

Recomendación:

La empresa deberá generar y documentar un plan de continuidad del negocio cuyo objetivo será proporcionar los mecanismos de reacción ante posibles interrupciones, fallas o desastres en la empresa.

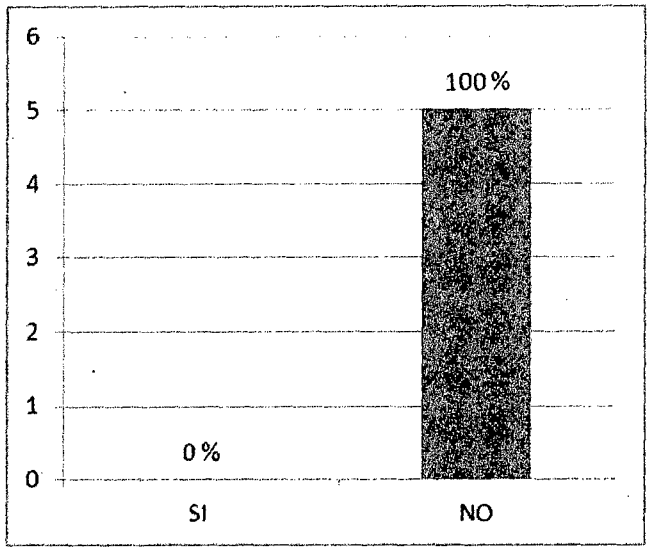


Gráfico N° 10: Evaluación de encuesta de Anexo N°10

Elaboración: Propia

4.2.11 EVALUACIÓN DE LA CONFORMIDAD (Anexo N° 11)

Problema N° 1:

La empresa no ha implementado controles para el cumplimiento normativo del uso del software licenciado por lo cual no existe un procedimiento de control permanente que garantice que los usuarios no instalen productos ilegales y que permita al área de informática conocer los productos de software instalados en las pc's de la empresa.

Recomendación:

Se deberían definir y documentar todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información.

Se debería buscar el asesoramiento sobre requisitos legales específicos de los asesores legales de la organización, o de profesionales del derecho calificados.

Problema N° 2:

La empresa no cuenta con un personal responsable, el cual debe mantenerse actualizado sobre las normas emitidas por la Oficina Nacional de Gobierno Electrónico.

Recomendación:

La empresa debe contar con una persona responsable del cumplimiento de las normas emitidas por la ONGEI, según los procedimientos de control establecidos por la misma.

Se debe contar con un control del cumplimiento de normas sobre la propiedad intelectual (licenciamiento de software).

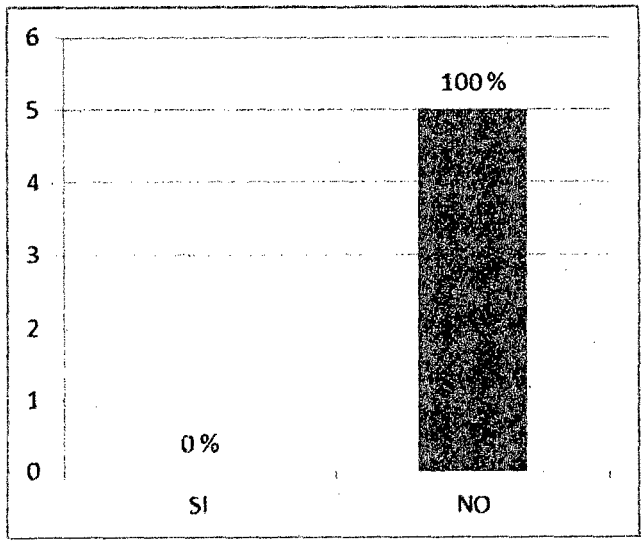


Gráfico N° 11: Evaluación de encuesta de Anexo N°11

Elaboración: Propia

4.3 DESARROLLO DEL ANÁLISIS DE RIESGOS:

El presente análisis de riesgos fue desarrollado con el propósito de determinar cuáles de los activos de la empresa tiene mayor vulnerabilidad ante factores externos o internos que puedan afectarlos, identificando las causas potenciales que faciliten o impidan alcanzar los objetivos y la probabilidad de su ocurrencia.

Para generar esta información se desempeñaron las siguientes actividades:

1. Listado de los activos de la empresa
2. Asignación de prioridades a los activos
3. Definición de factores de riesgo
4. Descripción de consecuencias
5. Asignación de probabilidades de ocurrencia de los factores de riesgo
6. Cálculo de niveles de vulnerabilidad

1. **Listado de los activos de la Empresa:** Se evaluaron los distintos activos físicos y de software de la empresa, generando un inventario de aquellos que son considerados como vitales para su desenvolvimiento seguro, éstos son:
   - Servidores y switch.
   - Base de datos.
   - Sistemas operativos.
   - Backup.
   - Datos de configuración.
   - Administrador de Centro de Cómputo
   - Red, Cableado Red LAN
   - Red eléctrica
   - Usuarios.
   - Hardware (teclado, monitor, unidades de discos, etc.)
   - Insumos (cartuchos de tinta, tóner, papel, etc.)
   - Datos de usuarios.

2. **Asignación de prioridades a los activos**: Al listado de activos se le ha asignado un valor ponderado en una escala del 1 al 10 de acuerdo a la importancia que tienen en la empresa. Esta importancia es un valor relativo que refleja el nivel de impacto que puede tener la empresa si un incidente afecta a los activos.

N°	ACTIVOS	Nivel de Importancia (1-10)
1	Servidores y switch	10
2	Base de datos	10
3	Sistemas operativos	10
4	Backup.	9
5	Datos de configuración	8
6	Administrador de centro de cómputo	8
7	Cableado de red LAN	8
8	Red	8
9	Usuarios	5
10	Hardware (estaciones de trabajo, impresoras de red)	3
11	Insumos (cartuchos de tinta, tóner, papel, etc)	2
12	Datos de usuarios	1

Tabla N° 05: Asignación de prioridades a los activos de la empresa

3. **Definición de factores de riesgo:** Los factores de riesgo son las amenazas que pueden afectar a los activos. Se ha realizado un estudio de los posibles riesgos a los cuales se les ha calificado, indicando la probabilidad de que éstas ocurran, en una escala del 1 al 3: Bajo (1), Medio (2) y Alto (3).

   Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en la empresa y acontecimientos ocurridos.

FACTORES DE RIESGO	PROBA B.
Abuso de puertos para el mantenimiento remoto	1
Acceso no autorizado a datos (borrado, modificación, etc.)	2
Administración impropia del sistema	2
Ancho de banda insuficiente	1
Aplicaciones sin licencia	3
Ausencia o falta de segmentación	1
Borrado, modificación o revelación desautorizada o inadvertida de información	3
Complejidad en el acceso a la red del sistema	1
Condiciones de trabajo adversas	1
Conexión de cables inadmisibles	1
Configuración inadecuada de componentes de la red	1
Conocimiento insuficiente de los documentos de requerimientos en el desarrollo.	2
Copia no autorizada de un medio de datos	2
Corte de luz o variaciones de voltaje	3
Daño de cables inadvertido	1
Descripción de archivos inadecuada	1
Destrucción negligente de equipos o datos	1
Destrucción o mal funcionamiento de un componente	1
Documentación deficiente	3
Documentación insuficiente o faltante, Funciones no documentadas	3

Entrada sin autorización a ambientes	2
Entrenamiento de usuarios inadecuado	2
Errores de configuración y operación	1
Errores de software	1
Factores Ambientales	1
Falla de Base de Datos	1
Falla del sistema	1
Falta de auditorías	3
Falta de autenticación	1
Falta de confidencialidad	1
Falta de cuidado en el manejo de la información (Ejm. Passwoard)	2
Falta de espacio de almacenamiento	1
Interferencias	1
Impresoras o directorios compartidos	1
Límite de vida útil – máquinas obsoletas	1
Longitud de los cables de red excedida	1
Mal interpretación	2
Mal mantenimiento	1
Mal uso de derechos del administrador	3
Mala integridad de los datos	1
Mantenimiento inadecuado o ausente	2
Medios de datos no están disponibles cuando son necesarios	1
Pérdida de Backups	3
Pérdida de confidencialidad en datos privados y de sistema	1

Pérdida de confidencialidad o integridad de datos como resultado de un error humano en el sistema	2
Pérdida de datos	1
Poca adaptación a cambios en el sistema	1
Reducción de velocidad de transmisión	1
Recursos escasos	1
Riesgo por el personal de limpieza o personal externo	1
Robo	2
Sabotaje	1
Seguridad de base de datos deficiente	1
Software desactualizado	1
Transferencia de datos incorrectos o no deseados	1
Transporte inseguro de medios de datos	1
Uso descontrolado de recursos	1
Uso sin autorización	1
Virus	3

Tabla N° 06: Factores de Riesgo

4. **Descripción de consecuencias:** Teniendo presente el listado anterior, se generó una descripción de las consecuencias que podría sufrir la empresa si los activos son afectados por sus respectivos factores de riesgo , detallando la manera en que se protege al activo contra este ataque en particular, y puntualizando en qué grado son efectivas estas medidas.

   Efectiva (e), deficiente (d), mejorable (m).

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Servidores y switch	Acceso no autorizado	Robo, modificación de información	Control de acceso lógico	m
	Corte de luz o variaciones de voltaje	Falta de sistema		d
	Destrucción de un componente	Pérdida de tiempo por necesidad de reemplazo		d
	Error de configuración	Aumento de vulnerabilidades e inestabilidad en el sistema	Mantenimiento por personal de Soporte.	e
	Factores Ambientales	Falta de sistema y destrucción de equipos	Buen diseño del edificio	m
	Límite de vida útil – Máquinas Obsoletas	Deterioro en la performance del sistema	Equipamiento actual	m
	Mal mantenimiento	Interrupciones en el funcionamiento del sistema	Mantenimiento interno, sólo mantenimiento correctivo	m

	Modificación no autorizada de datos	Inconsistencia de datos, mala configuración , fraude	Controles de acceso lógico al servidor	m
	Robo	Pérdida de equipamiento o información		d
	Virus	Fallas generales del sistema y en la red	Herramientas antivirus	m

Tabla N° 07 : Activo - Servidores y Switch

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Base de Datos	Copia no autorizada de un medio de datos	Divulgación de información	Controles lógicos	m
	Errores de software	Inconsistencia en los datos	Backups de los datos	m
	Falla de Base de datos	Inconsistencia en los datos	Backups de los datos	m

	Mala integridad de los datos	Inconsistencias y redundancia de datos	Controles en las aplicaciones desarrolladas	m
	Pérdida de backups	Incapacidad de restauración		d
	Pérdida de confidencialidad en datos privados y de sistema	Divulgación de información	Controles de accesos lógicos a datos	m
	Impresoras o carpetas compartidas	Divulgación de información	Controles lógicos	m
	Robo	Divulgación de información	Controles lógicos	m
	Sabotaje	Pérdida o modificación de datos, pérdida de tiempo y productividad	Backups y Controles lógicos	m
	Transferencia de datos incorrectos	Inconsistencia de datos	Controles lógicos	m
	Virus	Pérdida, modificación o divulgación de datos, pérdida de tiempo y productividad	Herramientas antivirus	m

Tabla N° 08: Activo – Base de Datos

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Sistemas Operativos	Error de configuración	Mal funcionamiento de los sistemas	Existe personal de mantenimiento	m
	Falla del sistema	Falta de sistema y posibles demoras	Backups	m
	Falta de confidencialidad	Divulgación de información	Controles lógicos	e
	Pérdida de datos	Divulgación de información	Backups	m
	Software desactualizado	Probabilidad incremental y mal funcionamiento de sistemas	Mantenimiento por área de sistemas	m
	Virus	Inestabilidad y mal funcionamiento de sistemas	Herramientas antivirus	m

Tabla N° 09: Activo - Sistemas operativos

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Backup	Copia no autorizada a un medio de datos	Robo de información	Controles de acceso lógico al servidor.	m
	Errores de software	Error en la generación o en la copia de backups a medios externos		d
	Falta de espacio de almacenamiento	Falla en la generación del Backup	Existencia de Cds para la copia.	m
	Mala integridad de los datos resguardados	Errores durante la restauración de datos	Numerosas copias de respaldo por posibles errores.	m
	Pérdida de Backups	Falta de datos, incapacidad de restaurarlos y divulgación de información		d
	Robo	Incapacidad de restaurarlos y divulgación de información		d
	Sabotaje	Pérdida o robo de información		d

	Virus	Pérdida de datos de Backup	Herramientas antivirus	m

Tabla N° 10: Activo - Backup

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Datos de configuración	Copia no autorizada a un medio de datos	Robo de información	Controles de acceso lógico a los sistemas	e
	Impresoras o carpetas compartidas	Divulgación o robo de información	Prohibición de la impresión	m
	Mala integridad de los datos	Inconsistencia de información	Controles de integridad en la transmisión, en el ingreso de datos	m
	Pérdida de datos en tránsito	Divulgación de información	Utilización de protocolos seguros en la transmisión.	m

	Sabotaje	Pérdida o robo de información	Utilización de protocolos seguros en la transmisión	m
	Virus	Pérdida, modificación o divulgación de datos, pérdida de tiempo y productividad.	Herramientas antivirus	m

Tabla N° 11: Activo – Datos de configuración

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Administrador de Centro de Cómputo	Administración impropia del sistema (responsabilidades y roles del personal de sistemas)	Asignación de responsabilidades impropia.		d
	Errores de configuración y operación del sistema	Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades.	El mantenimiento diario lo realiza el administrador de centro de cómputo	m

	Falta de auditorías en sistema operativo	Imposibilidad del seguimiento de usuarios y de la generación de reportes.		d
	Mal uso de derechos de administrador	Mala distribución de los permisos y de las cuentas del administrador.	El administrador de base de datos realiza la distribución de cuentas usuario	m

Tabla N° 12: Activo – Administrador de Centro de Cómputo

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Cableado de red LAN	Ancho de banda insuficiente	Transmisión pesada en la red o imposibilidad de utilizar el sistema.	Utilización de protocolo seguro en la transmisión.	e
	Conexión de cables inadmisible	Pinchaduras de cables, robo de datos.	Cableado estructurado aplicado en el tendido de la empresa	e

	Daño o destrucción de cables o equipamiento inadvertido	Pinchaduras de cables, robo de datos.		d
	Factores Ambientales	Interferencias o daños de equipamiento	Buen diseño de edificio.	m
	Interferencias	Errores en los datos de transmisión o imposibilidad de utilizar el sistema.		d
	Límite de vida útil de equipos	Equipos obsoletos e imposibilidad de utilizar el sistema	Mantenimiento por personal - soporte tec.	e
	Longitud de los cables de red excedida	Transmisión lenta o con interferencias, o imposibilidad de utilizar el sistema.	Mantenimiento por administrador de centro de cómputo	e
	Mal mantenimiento	Errores de transmisión o interrupción del servicio de la red	Mantenimiento del cableado estructurado realizado por personal de soporte técnico	e
	Reducción de velocidad de transmisión	Pérdida de tiempo de los usuarios, o imposibilidad de utilizar el sistema	Utilización de protocolo seguro en la transmisión.	e

	Riesgo por personal de limpieza o personal externo	Daño en cables o equipos, interrupción del sistema	Cables y equipos protegidos, fuera de la vista y el alcance de terceros.	e

Tabla N° 13: Activo – Cableado de red LAN

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Red	Abuso de puertos para el mantenimiento remoto	Posibles intrusiones y robo o divulgación de información	Política de configuración de puertos restringida.	m
	Ausencia o falta de segmentación	Tramos de red extensos y dificultades en la comunicación	Red segmentada física y lógicamente por sectores	e
	Complejidad en el diseño de red del sistema	Dificultad en la administración y en el mantenimiento	Diseño de red con topología estrella	e
	Configuración inadecuada de	Errores de transmisión, interrupción del	Equipamiento de red	e

	componentes de red	servicio de red.	configurado por personal de soporte técnico.	
	Errores de configuración y operación	Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades	El mantenimiento diario lo realiza el administrador de centro de cómputo.	m
	Falta de autenticación	Posibles intrusiones y robo o divulgación de información	Controles de acceso a datos y a equipos	m

Tabla N° 14: Activo - Red

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Usuarios	Acceso no autorizado a datos	Divulgación o robo de información	Controles de acceso lógico a datos en las aplicaciones.	e
	Borrado, modificación o	Inconsistencia de datos o datos faltantes	Controles lógicos a datos.	m

	revelación desautorizada o inadvertida de información			
	Condiciones de trabajo adversas	Predisposición a distracción, bajo rendimiento de usuarios	Ambiente de trabajo cómodo.	e
	Destrucción de un componente de hardware	Pérdida de tiempo por necesidad de reemplazo	Reemplazo emergente de componentes.	m
	Destrucción negligente de datos	Pérdida de información	Controles lógicos a datos en las aplicaciones	e
	Documentación deficiente	Mayor probabilidad de errores por falta de instrucciones		d
	Entrada sin autorización a habitaciones	Robo de equipos o insumos, divulgación de datos		d
	Entrenamiento de usuarios inadecuado	Predisposición a errores y bajo rendimiento de usuarios	Capacitación usuarios en el uso del sistema.	m
	Falta de auditorías	Predisposición a un rendimiento mediocre y		d

		falta de concienciación sobre responsabilidades y seguridad		
	Falta de cuidado en el manejo de la información (Ej. Password)	Divulgación de datos	Insistencia con respecto al uso discreto de datos.	m
	Mal uso de derechos de administrador (sesiones abiertas)	Divulgación o robo de información, sabotaje interno.		d
	Pérdida de confidencialidad o integridad de datos como resultado de un error humano	Error en la información	Controles lógicos de acceso a datos y de integridad de datos de entrada al sistema	m

Tabla N° 15: Activo – Usuarios

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Hardware (Teclado, monitor, unidades de discos, etc.)	Corte de luz o variaciones de voltaje	Interrupción del funcionamiento de equipos		d
	Destrucción o mal funcionamiento de un componente	Interrupción de la tarea del usuario	Componente de respaldo	m
	Límite de vida útil	Avería de equipos	Equipos de respaldo	m
	Factores Ambientales	Destrucción o avería de equipos	Equipos de respaldo	m
	Mal mantenimiento	Avería de equipos e incremento en el costo de equipamiento de respaldo	Mantenimiento realizado por personal de soporte.	m
	Robo	Pérdida de equipamiento e interrupción de la tarea del usuario		d

Tabla N° 16: Activo - Hardware

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Insumos (cintas, cartuchos de tinta, toner, papel, etc.)	Factores ambientales	Destrucción de insumos	Insumos de respaldo	m
	Límite de vida útil	Destrucción o avería de insumos	Insumos de respaldo	m
	Uso descontrolado de recursos	Incremento no justificado del gasto de insumos		d
	Robo	Pérdida de insumos e incremento en el gasto		d
	Transporte inseguro de medios de datos	Pérdida de datos, de insumos e incremento en el gasto.	Tarea asignada al administrador del centro de cómputo.	m

Tabla N° 17: Activo - Insumos

Nombre del Activo	Factor de Riesgo	Consecuencias	Tipo de protección	Efectividad
Datos de Usuarios	Falta de espacio de almacenamiento	Retraso de las actividades.	Capacidad de almacenamiento sobredimensionada	e
	Medios de datos no están disponibles cuando son necesarios	Retraso de las actividades.	Permanente disponibilidad de éstos medios por personal del área de sistemas	e
	Pérdida de backups	Pérdida de datos del usuario y retraso de la tarea	Controles de acceso lógico al equipo usado para tal copias de respaldo	m
	Pérdida de confidencialidad en datos privados y de sistema	Divulgación de información	Controles de acceso lógico a la PCs de los usuarios	m
	Impresoras o carpetas compartidas	Divulgación de información		d

	Robo	Divulgación de información	Controles de acceso lógico a los equipos	m
	Sabotaje	Pérdida, modificación o divulgación de datos	Controles de acceso lógico a equipos y copias de respaldo de los datos	m
	Virus	Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad	Herramientas antivirus	m

Tabla N° 18: Activo – Datos de Usuarios

5. **Asignación de probabilidades de ocurrencia de los factores de riesgo:** Teniendo en cuenta los datos arriba mencionados fue posible estimar la probabilidad de ocurrencia que cada uno de los factores de riesgo representaba con respecto a los activos listados, considerando para esta estimación las medidas a tomar por la empresa para mitigar su acción.

   a) **Probabilidad de Ocurrencia**: Representan la probabilidad que ocurran los factores de riesgo mencionados, en una escala del 1 al 3. Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en la organización.

   b) **Porcentaje de la Probabilidad del Riesgo**: Se calcula el porcentaje de probabilidad de que ocurra un determinado factor de riesgo, con respecto a la cantidad de factores de riesgo intervinientes para dicho activo. Esto es debido a que cada activo está afectado por un número diferente de riesgos posibles, de manera que éste cálculo sirve para obtener un porcentaje de probabilidades equilibrado por igual para cualquier activo, independientemente de la cantidad de factores de riesgo que lo afectan.

   c) **Niveles de Vulnerabilidad**: Interviene el nivel de importancia, multiplicando al porcentaje de probabilidad del riesgo. De ésta forma se obtiene el nivel de vulnerabilidad de cada activo con respecto a un factor de riesgo. La suma de éstos valores es el nivel de vulnerabilidad total que corresponde a cada activo

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
1	Servidores y switch	10	Acceso no autorizado	2	20.00	200.00
			Corte de luz o variación de voltaje	3	30.00	300.00
			Destrucción de un componente	1	10.00	100.00
			Error de configuración	1	10.00	100.00
			Factores Ambientales	1	10.00	100.00
			Límite de Vida útil, Máquinas Obsoletas	1	10.00	100.00
			Mal mantenimiento	1	10.00	100.00
			Modificación no autorizada de datos	1	10.00	100.00
			Robo	2	20.00	200.00
			Virus	3	30.00	300.00
Cantidad de Factores de Riesgo = 10						1600.00

Tabla N° 19: Cálculo de la vulnerabilidad para Activo-Servidores y switch

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
2	Base de Datos	10	Copia no autorizada de un medio de datos	2	18.18	181.80
			Errores de software	1	9.09	90.90
			Falla de Base de datos	1	9.09	90.90
			Mala integridad de los datos	1	9.09	90.90
			Pérdida de backups	3	27.27	272.70
			Pérdida de confidencialidad en datos privados y de sistema	1	9.09	90.90
			Impresoras o directorios compartidos	1	9.09	90.90
			Robo	2	18.18	181.80
			Sabotaje	1	9.09	90.90
			Transferencia de datos incorrectos	1	9.09	90.90
			Virus	3	27.27	272.70
Cantidad de Factores de Riesgo = 11						1545.30

Tabla N° 20: Cálculo de la vulnerabilidad para Activo - Base de Datos

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
3	Sistemas operativos	10	Error de configuración	1	16.67	166.70
			Falla del sistema	1	16.67	166.70
			Falta de confidencialidad	1	16.67	166.70
			Pérdida de datos	1	16.67	166.70
			Software desactualizado	1	16.67	166.70
			Virus	3	50.00	500.00
Cantidad de Factores de Riesgo = 06						1333.50

Tabla N° 21: Cálculo de la vulnerabilidad para Activo – Sistemas Operativos

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
4	Backup	9	Copia no autorizada a un medio de datos	2	28.57	257.13
			Errores de software	1	14.29	128.61
			Mala integridad de los datos resguardados	1	14.29	128.61
			Pérdida de Backups	3	42.86	385.74
			Robo	2	28.57	257.13
			Sabotaje	1	14.29	128.61
			Virus	2	28.57	257.13
Cantidad de Factores de Riesgo = 7						1542.96

Tabla N° 22: Cálculo de la vulnerabilidad para Activo – Backup

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
5	Datos de configuración	8	Copia no autorizada a un medio de datos	2	33.33	266.64
			Impresoras o directorios compartidos	1	16.67	133.36
			Mala integridad de los datos	1	16.67	133.36
			Pérdida de datos en tránsito	1	16.67	133.36
			Sabotaje	1	16.67	133.36
			Virus	3	50.00	400.00
Cantidad de Factores de Riesgo = 6						1200.08

Tabla N° 23: Cálculo de la vulnerabilidad para Activo - Datos de configuración

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
6	Administra-dor de Centro de Cómputo	8	Administración impropia del sistema (responsabilidades y roles del personal de sistemas).	2	50.00	400.00
			Errores de configuración y operación del sistema.	1	25.00	200.00
			Falta de auditorías en sistema operativo	3	75.00	600.00
			Mal uso de derechos de administrador	3	75.00	600.00
Cantidad de Factores de Riesgo = 4						1800.00

Tabla N° 24: Cálculo de la vulnerabilidad para Activo – Administrador de Centro de Cómputo

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
7	Cableado de red	8	Ancho de banda insuficiente	1	10.00	80.00
			Conexión de cables inadmisible	1	10.00	80.00

	LAN		Daño o destrucción de cables o equipamiento inadvertido	1	10.00	80.00
			Interferencias	1	10.00	80.00
			Factores Ambientales	1	10.00	80.00
			Límite de vida útil de equipos	1	10.00	80.00
			Longitud de los cables de red excedida	1	10.00	80.00
			Mal mantenimiento	1	10.00	80.00
			Reducción de velocidad de transmisión	1	10.00	80.00
			Riesgo por personal de limpieza o personal externo	1	10.00	80.00
Cantidad de Factores de Riesgo = 10						800.00

Tabla N° 25 : Cálculo de la vulnerabilidad para Activo - Cableado de red LAN

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
8	Red	8	Abuso de puertos para el mantenimiento remoto	1	16.67	133.33
			Ausencia o falta de segmentación	1	16.67	133.33
			Complejidad en el diseño de red del sistema	1	16.67	133.33
			Configuración inadecuada de componentes de red	1	16.67	133.33
			Errores de configuración y operación	1	16.67	133.33
			Falta de autenticación	1	16.67	133.33
Cantidad de Factores de Riesgo = 6						799.98

Tabla N° 26: Cálculo de la vulnerabilidad para Activo – Red

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
9	Usuarios	5	Acceso no autorizado a datos	2	16.67	83.35
			Borrado, modificación o revelación desautorizada o inadvertida de información	3	25.00	125.00
			Condiciones de trabajo adversas	1	8.33	41.65
			Destrucción de un componente de hardware	1	8.33	41.65
			Destrucción negligente de datos	1	8.33	41.65
			Documentación deficiente	3	25.00	125.00
			Entrada sin autorización a habitaciones	2	16.67	83.35
			Entrenamiento de usuarios inadecuado	2	16.67	83.35
			Falta de auditorías	3	25.00	125.00
			Falta de cuidado en el manejo de la información.(Ejm. Passwoard)	2	16.67	83.35
			Mal uso de derechos de administrador(sesiones	2	16.67	83.35

			abiertas)			
			Pérdida de confidencialidad o integridad de datos como resultado de un error humano	2	16.67	83.35
Cantidad de Factores de Riesgo = 12						1000.05

Tabla N° 27: Cálculo de la vulnerabilidad para Activo–Usuarios

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
10	Hardware(teclado, monitor, unidades de discos, etc)	3	Corte de luz o variaciones de voltaje	3	50.00	150.00
			Destrucción o mal funcionamiento de un componente	1	16.67	50.01
			Factores Ambientales	1	16.67	50.01
			Límite de vida útil	1	16.67	50.01
			Mal mantenimiento	1	16.67	50.01
			Robo	2	33.33	99.99
Cantidad de Factores de Riesgo = 6						450.03

Tabla N° 28: Cálculo de la vulnerabilidad para Activo – Hardware

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
11	Insumos (cartuchos de tinta, toner, papel, formularios, etc.)	2	Límite de vida útil	1	16.67	33.34
			Factores Ambientales	1	16.67	33.34
			Recursos escasos	1	16.67	33.34
			Uso descontrolado de recursos	1	16.67	33.34
			Robo	2	3333	66.66
			Transporte inseguro de medios de datos	1	16.67	33.34
Cantidad de Factores de Riesgo = 6						233.36

Tabla N° 29: Cálculo de la vulnerabilidad para Activo - Insumos

N° Activo	Nombre del Activo	Nivel de importancia	Factor de Riesgo	Prob. de Ocurrencia	% Prob. Riesgos	Nivel de Vulnerabilidad
12	Datos de usuarios	1	Falta de espacio de almacenamiento	1	12.5	12.5
			Medios de datos no están disponibles cuando son necesarios	1	12.5	12.5
			Pérdida de backups	3	37.5	37.5
			Pérdida de confidencialidad en datos privados y de sistema	1	12.5	12.5
			Impresoras o directorios compartidos	1	12.5	12.5
			Robo	2	25	25
			Sabotaje	1	12.5	12.5
			Virus	3	37.5	37.5
Cantidad de Factores de Riesgo = 8						162.5

Tabla N° 30: Cálculo de la vulnerabilidad para Activo - Datos de usuario

6. **Cálculo de niveles de vulnerabilidad:** Una vez identificados los riesgos, se procedió a su análisis. Con toda la información recolectada, se determinó el nivel de vulnerabilidad que se asocia con cada activo listado.

   En el cuadro se listan los activos, ordenados de forma descendente de acuerdo al riesgo que corren dichos activos. De tal forma se puede apreciar que el recurso que más debe protegerse es el activo: Administrador de Centro de Cómputo, quien es el encargado de mejorar la calidad de la gestión del servicio informático, (planeación, organización, dirección y control).

Nombre de Activos	Nivel de Vulnerabilidad
1. Administrador de Centro de Cómputo	1800.00
2. Servidores y switch	1600.00
3. Base de Datos	1545.30
4. Backup	1542.96
5. Sistemas Operativos	1333.50
6. Datos de configuración	1200.08
7. Usuarios	1000.05
8. Cableado de Red LAN	800.00
9. Red	799.98
10. Hardware (teclado, monitor, etc)	450.03
11. Insumos (cartuchos de tinta, toner, papel, etc)	233.36
12.Datos de usuarios	162.50

Tabla N° 31: Resumen de los Niveles de Vulnerabilidad de los Activos Informáticos

4.4 FORMULACIÓN DEL PLAN DE SEGURIDAD INFORMÁTICO

4.4.1 POLÍTICA DE SEGURIDAD

La Gerencia deberá crear, aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados de manera apropiada, entendible y accesible.

Para la redacción de este documento se le propone tener como base a la Norma ISO/IEC 27002, el cual contendrá la siguiente información:

- Definición, alcance e importancia de la seguridad de la información como mecanismo que permite compartir la información.
- Proteger los recursos de información de la empresa y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Mantener la política de seguridad de la empresa actualizada, a efectos de asegurar su vigencia y nivel de eficacia.
- Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes.
- Sanciones previstas por incumplimiento de las disposiciones establecidas por las políticas de seguridad de la información el cual tendrá diversas

sanciones, conforme a la magnitud y característica del aspecto no cumplido.

4.4.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.4.2.1 Comité de Seguridad de la Información: Se propone la creación de este comité integrado por representantes de áreas sustantivas de la empresa destinado a garantizar la seguridad de la información, la cual estará conformado por las siguientes personas:

- Gerente
- Un representante del área de informática
- Un representante del área usuaria

Las funciones del Comité serán:

a) Elaborar, documentar, actualizar y proponer a la máxima autoridad de la empresa para su aprobación, las políticas y procedimientos relativos a la seguridad de la información.

b) Monitorear el cumplimiento de la política de seguridad de la empresa.

c) Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la empresa frente a posibles amenazas, sean internas o externas.

d) Coordinar el análisis de riesgos, planes de contingencia y planes de continuidad.

e) Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como el monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de la empresa.

f) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

g) Coordinar el proceso de administración de la continuidad de las operaciones de los sistemas de tratamiento de información de la empresa frente a interrupciones imprevistas.

h) Aprobación de las iniciativas principales para mejorar la seguridad de la información.

4.4.2.2 Asignación de responsabilidades en materia de seguridad de la información.

La empresa deberá contar con un "Responsable de Seguridad Informática", quien tendrá a cargo la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política. Además será quien difunda la importancia de

la Seguridad de la información entre todo el personal de la empresa.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades que surjan de los procesos de seguridad que se detallan a continuación, indicando en cada caso el/los responsable/s del cumplimiento de los aspectos de esta política aplicables a cada caso:

a) Seguridad del Personal

b) Seguridad Física y Ambiental

c) Seguridad en las Comunicaciones y las Operaciones.

d) Control de Accesos

e) Seguridad en el Desarrollo y Mantenimiento de Sistemas

f) Planificación de la Continuidad Operativa

Así mismo, el Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades de los propietarios de la información que se definan, quienes serán los responsables de las unidades organizativas a cargo y en poner en conocimiento la importancia respecto a la seguridad de la información.

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo,

conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al responsable de seguridad informática.

PROPIETARIO DE INFORMACION:

Los propietarios de información son: el Gerente y Jefes de áreas, las cuales son responsables de la información que se genera y se utiliza en las operaciones de su respectiva oficina. Las áreas de la empresa deben ser conscientes de los riesgos de tal forma que sea posible tomar decisiones para disminuir los mismos.

4.4.2.3 Asesoramiento Especializado en Materia de Seguridad de la información.

El responsable de seguridad informática será el encargado de coordinar los conocimientos y las experiencias disponibles en el tema de seguridad informática, a fin de brindar ayuda en la toma de decisiones en esta materia. Éste podrá obtener asesoramiento de otros organismos especializados en temas relativos a la seguridad informática como la *Oficina Nacional de Gobierno Electrónico e Informático (ONGEI).*

4.4.2.4 Seguridad Frente al Acceso por Parte de Terceros

Cuando exista la necesidad de otorgar información de la empresa a terceras partes, el responsable de seguridad

informática y el propietario de la información, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información de la empresa.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

4.4.2.5 Plan Operativo informático

La empresa contará con un Plan Operativo Informático, en el cual se definen las actividades y proyectos a realizar durante un año, de acuerdo a las metas y objetivos de la empresa.

4.4.3 GESTION DE ACTIVOS

4.4.3.1 Inventario de Activos

El responsable de la seguridad informática será el encargado de elaborar el inventario y mantenerlo actualizado ante cualquier modificación de la información registrada, tanto de hardware como de software.

Cada activo debe ser claramente identificado y clasificado en cuanto a seguridad por su propietario debiendo estar documentadö.

Ejemplos de activos asociados a sistemas de información son los siguientes:

-**Información:** Documentos, informes, libros, manuales, correspondencias, patentes, estudios de mercados, programas, códigos fuentes, líneas de comandos, reportes, archivos, planillas de pago, planes de negocio, etc.

-**Equipos que la soportan**: Dentro de ellos tenemos:

*Software.-Programas de computadora para la automatización de los procesos de la empresa. (Aplicaciones comerciales, programas institucionales, sistemas operativos, otros).

*Hardware.- Infraestructura tecnológica que brinda soporte a la información durante su uso, tránsito y almacenamiento.

*Organización.- Aspectos que conforman la estructura física salas de servidores, armarios, archivadores, salas de trabajo,

etc.) y organizativa de la empresa (Áreas, funciones y funcionarios, flujo de información, flujo de trabajo). Organización lógica y física del personal de la empresa.

***Usuarios:** personas que utilizan la estructura tecnológica y de comunicación de la empresa y manejan la información.

Se busca formar el hábito de la seguridad para que los usuarios tomen conciencia de las vulnerabilidades.

4.4.3.2 Clasificación del acceso a la información :

Toda la información en la empresa debe ser clasificada como restringida, confidencial, uso interno o general.

Restringida: Información con mayor grado de sensibilidad; el acceso a esta información debe ser autorizado con mucho cuidado.

Confidencial: Información sensible que solo debe ser divulgada a aquellas personas que la necesiten para el cumplimiento de sus funciones.

Uso Interno: Datos generados para facilitar las operaciones diarias; deben de ser manejados de una manera discreta, pero no requiere de medidas elaboradas de seguridad.

General: Información que es generada específicamente para su divulgación a la población general de usuarios.

- La clasificación asignada a un tipo de información, sólo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.

- La información que existe en más de un medio (por ejemplo, documento fuente, registro electrónico, reporte o red) debe de tener la misma clasificación sin importar el formato.

- La información debe de ser examinada para determinar el impacto en la empresa, si fuera divulgada o alterada por medios no autorizados. Por ejemplo de información sensible: Datos que proveen acceso a información o servicios: autenticación, contraseñas; datos protegidos por legislación de privacidad vigente: Registros del personal.

4.4.3.3 Aplicación de Controles para la información clasificada :

Las medidas de seguridad a ser aplicadas a los activos de información clasificados de acuerdo a su importancia, incluyen pero no se limitan a las siguientes:

A) Información de la Empresa en formato digital:

- Todo contenedor de información en medio digital (CD's, cintas de backup, usb, etc.) debe presentar una etiqueta con la clasificación correspondiente.

- La información en formato digital clasificada como de acceso "General", puede ser almacenada en cualquier sistema de la

empresa. Sin embargo no se debe mezclar información General con información de otra clasificación.

- Todo usuario, antes de transmitir información clasificada como "Restringida" o "Confidencial", debe asegurarse que el destinatario de la información esté autorizado a recibir dicha información.

- Todo usuario que requiere acceso a información clasificada como "Restringida" o "Confidencial", debe ser autorizado por el propietario de la misma. Las autorizaciones de acceso a éste tipo de información deben ser documentadas.

- La clasificación asignada a un tipo de información, sólo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.

- Información en formato digital, clasificada como "Restringida", debe ser encriptada con un método aprobado por el responsable de la seguridad de la información, cuando es almacenada en cualquier medio (disco duro, disquetes, Cds, etc.)

- Es recomendable el uso de técnicas de encriptación para la información clasificada como "Restringida" o "Confidencial", transmitida a través de la red de datos de la Empresa.

• Todo documento en formato digital, debe presentar la clasificación correspondiente en la parte superior (cabecera) e inferior (pie de página) de cada página del documento.

• Los medios de almacenamiento, incluyendo discos duros de computadoras, que albergan información clasificada como "Restringida", deben ser ubicados en ambientes cerrados diseñados para el almacenamiento de dicho tipo de información. En lugar de protección física, la información clasificada como "Restringida" podría ser protegida con técnicas de encriptación aprobadas por la empresa.

B) Información de la empresa en formato no digital:

• Todo documento o contenedor de información debe ser etiquetado como "Restringida", "Confidencial", de "Uso Interno" o de "Acceso General", dependiendo de la clasificación asignada.

• Todo documento que presente información clasificada como "Confidencial" o "Restringida", debe ser etiquetado en la parte superior e inferior de cada página con la clasificación correspondiente.

• Todo documento clasificado como "Confidencial" o "Restringido", debe contar con una carátula en la cual se muestre la clasificación de la información que contiene.

• Los activos de información correspondiente a distintos niveles de clasificación, deben ser almacenados en distintos contenedores.

- El ambiente donde se almacena la información clasificada como "Restringida", debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal formalmente autorizado. El personal de limpieza debe ingresar al ambiente acompañado por personal autorizado.

- Sólo el personal formalmente autorizado debe tener acceso a información clasificada como "Restringida" o "Confidencial".

- Los usuarios que utilizan documentos con información "Confidencial" o "Restringida" deben asegurarse:

  - Almacenarlos en lugares adecuados.
  - Evitar que usuarios no autorizados accedan a dichos documentos.
  - Destruir los documentos si luego de su utilización dejan de ser necesarios.

4.4.4 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Las personas son necesarias para que trabajen en las computadoras pero también es cierto que la mayor amenaza para los sistemas de seguridad de una empresa es la deshonestidad y negligencia de sus propios empleados. Los gerentes deben poner mucha atención al personal que contratan para puestos con acceso a los sistemas computarizados de

información y de datos delicados ya que alguien totalmente negligente puede causar tanto daño como alguien que sea deshonesto por naturaleza

El responsable del área de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los compromisos de confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El Responsable de Seguridad Informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información y a la coordinación de emergencias en Redes informáticas.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad Informática maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

4.4.4.1 Puesto de Trabajo

El Responsable del Área de Recursos Humanos tendrá en cuenta los siguientes aspectos relativos a la seguridad para la

elaboración e implementación de un procedimiento de reclutamiento de personal:

a) **Definición del puesto**: Para cada nueva vacante se debe definir la criticidad del puesto a cubrir según su responsabilidad y la información que maneja.

b) **Selección:** En la selección de candidatos a puestos críticos se deben comprobar los antecedentes penales y las referencias profesionales.

c) **Contrato:** El contrato laboral debe incluir los correspondientes acuerdos de confidencialidad, propiedad intelectual y protección de datos.

d) **Comienzo:** Durante los primeros días de trabajo, es recomendable que el empleado asista a unas sesiones de formación y capacitación donde se brinde conocimiento sobre la normativa interna y de seguridad de la empresa, reciba el manual de normativa interna y firme el compromiso de cumplimiento del mismo.

e) **Accesos:** En las sesiones de formación de seguridad de la empresa el empleado conocerá sus obligaciones de seguridad tales como la protección de sus claves de acceso, uso adecuado del email e internet, clasificación de la información, etc.

   El empleado deberá recibir el manual de normativa interna y firme el compromiso de cumplimiento del mismo. Este trámite

establece formalmente las normas internas y garantiza que el empleado conoce la normativa existente.

El acceso a la información y sistemas informáticos deben ser solicitados siempre por el responsable directo del empleado al área de sistemas. Dichos accesos deben ser siempre justificables por la labor que se va a realizar.

4.4.4.2 Credenciales de identificación

Cualquier persona que ingrese a la organización deberá llevar una credencial.

Estas credenciales pueden clasificarse de la siguiente manera:

- Normal o definitiva: para el personal permanente de planta.
- Temporaria: para personal recién ingresado.
- Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.
- Visitas.

4.4.4.3 Capacitación Continua y concientización al personal

El personal debe recibir periódicamente información actualizada sobre la seguridad y el uso apropiado de las computadoras. Esta capacitación continua es una oportunidad de explicar las buenas costumbres, recordarles a los usuarios las amenazas y las consecuencias de las fallas, y proporcionar un foro para discutir las preguntas y preocupaciones del personal.

Los colaboradores de los administradores de sistemas deben tener la oportunidad de capacitarse continuamente.

Esto incluye asistir a reuniones profesionales y seminarios, suscribirse a revistas técnicas y gremiales, y comprar libros de referencia y otros materiales.

Deben tener tiempo para leer y usar este material y recibir incentivos para dominarlo.

Junto con la capacitación continua puede considerarse un programa de concientización continua.

Esto incluye la colocación de avisos acerca de las buenas costumbres, usar mensajes diarios con consejos y recordatorios, realizar un "día de concientización" cada tres meses y llevar a cabo otros eventos que eviten que la seguridad caiga en el olvido.

Se debe pensar en el costo de las actividades de concientización y presupuestarlas.

4.4.4.4 Comunicación de Incidentes Relativos a la Seguridad

Los incidentes relativos a la seguridad serán comunicados a través de canales apropiados tan pronto como sea posible al responsable de Seguridad Informática. Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento deberá contemplar que ante la

detección de un supuesto incidente o violación de la seguridad, el responsable de seguridad informática sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente y se encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

4.4.4.5 Comunicación de Debilidades en Materia de Seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.

4.4.4.6Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:

a) Registrar los síntomas del problema y los mensajes que aparecen en pantalla.

b) Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.

c) Alertar inmediatamente al Responsable de Seguridad Informática o del Activo de que se trate.

La recuperación será realizada por personal experimentado, adecuadamente habilitado.

4.4.5 SEGURIDAD FÍSICA Y AMBIENTAL

4.4.5.1 CONTROL DE ACCESO FÍSICO AL ÁREA DE SISTEMAS O CÓMPUTO

La empresa utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. Asimismo en el área de servidores no existirán tuberías de agua, ni motores ni microondas que puedan ocasionar interferencia con tracción magnética.

4.4.5.2 CONTROLES DE ACCESO FÍSICO

- Se deberá restringir el acceso físico al área de sistemas a toda persona no autorizada, para reducir el riesgo de accidentes y actividades fraudulentas.
- Todo personal deberá usar credencial o ficha de identificación a fin de llevar un mejor control del ingreso y egreso del personal a la empresa.

- El personal ajeno al centro de cómputo llenará un formulario de datos personales, motivo de la visita, hora de ingreso y de egreso, etc. quienes durante su permanencia en el centro de cómputo portarán su credencial de visita asimismo serán acompañados por un empleado de la empresa.
- Se deberá registrar todos los ingresos y salidas de los empleados al área de informática, incluyendo el propio personal del área, quienes podrán permanecer en el área dentro del horario de trabajo. Además se contará con una cámara de video que se encargue de monitorear el área de sistemas.
- El área donde se encuentran los servidores, el switch central y demás equipos solo debe tener permitido el acceso a los administradores.
- La temperatura en el centro de cómputo no debe sobrepasar los 18° C y el límite de humedad no debe superar el 65% para evitar el deterioro. Asimismo se tendrá un equipo de Aire acondicionado sobre todo para la época de verano y evitar así el sobrecalentamiento de los equipos.
- Deben instalarse extintores para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.

- Se deberá contar con sensores contra Incendios, debiendo probarse regularmente para corroborar su funcionamiento.
- Deberá existir al menos una cámara de video para que pueda monitorear el área de sistemas. Las cintas deben ser guardadas para su posible análisis.
- La empresa deberá contar con personal de vigilancia las 24 horas del día.

4.4.5.3 CONTROL DE ACCESO A EQUIPOS

- Las lectoras de CD deberán deshabilitarse en aquellas máquinas en que no se necesiten.
- Las PC´s de la empresa deberán tener un password de administrador en el **BIOS**, que deberá gestionar el administrador del sistema.
- El jefe del área de sistemas o algún encargado designado por él, deberá realizar chequeos periódicos para comprobar:
  a) La correcta instalación de los dispositivos de los equipos, o su buen funcionamiento.
  b) sus números de series corresponden con los datos registrados por el administrador al momento de la instalación.
- Los servidores deberán apagarse automáticamente una vez que han cerrado la empresa.

- Se sugiere realizar un Plan de mantenimiento preventivo, consistente en limpieza, detección y corrección de fallas de hardware y software de: Servidores, CPU's, Monitores, impresoras y demás dispositivos; este programa permitirá minimizar el riesgo de presentarse un mantenimiento correctivo, evitando que su costo sea demasiado alto.
- Todos los disquetes, cintas, CD's, y otros dispositivos de almacenamiento de información incluyendo información impresa, que contengan datos sensibles deben ser guardados en un ambiente seguro cuando no sean utilizados.
- Los disquetes no deben ser expuestos a temperaturas altas o a elementos altamente magnéticos.

4.4.5.4 PROTECCIÓN DE OFICINAS, RECINTOS E INSTALACIONES

La empresa tendrá en cuenta la posibilidad de daño producido por un incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan las casas, zonas aledañas y cercanía al mar.

4.4.5.5 DESARROLLO DE TAREAS EN ÁREAS PROTEGIDAS

Para incrementar la seguridad de las áreas protegidas, se establecerán controles y lineamientos adicionales, que incluyan controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí.

4.4.5.6 UBICACIÓN Y PROTECCIÓN DEL EQUIPAMIENTO Y COPIAS DE SEGURIDAD

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

Asimismo se contará con los planos descriptivos documentados, los cuales contendrán la ubicación exacta de los puntos de red y el recorrido del cableado.

4.4.5.7 SUMINISTROS DE ENERGIA

La empresa contará con los respectivos equipos para abastecer de energía eléctrica ante posibles fallas en el suministro u otras anomalías eléctricas. Por ejemplo equipo electrógeno, ups, etc.

4.4.5.8 SEGURIDAD DEL CABLEADO

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.

4.4.5.9 MANTENIMIENTO DE EQUIPOS

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes, teniendo en cuenta a tal efecto:

a) La realización de tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del responsable del Área Informática.

b) El establecimiento de la práctica de que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

c) La registración de todas las fallas -supuestas y/o reales- y de todo el mantenimiento preventivo y correctivo realizado.

d) La registración del retiro de equipamiento para su mantenimiento de la sede de la empresa.

e) La eliminación de toda información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

4.4.6 GESTIÓN DE COMUNICACIONES Y OPERACIONES

La empresa evalúa la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la

documentación necesaria para la realización eficiente e ininterrumpida de esta transmisión, y los sistemas usados para la transmisión de datos de un entorno a otro.

4.4.6.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS

4.4.6.1.1 Documentación de los procedimientos operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta política y sus cambios serán autorizados por el responsable de la seguridad informática.

4.4.6.1.2 Control de Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El responsable de seguridad informática controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. Asimismo evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

4.4.6.2 PLANIFICACIÓN Y APROBACIÓN DE SISTEMAS

El Responsable del Área Informática, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, las cuales aprobará posteriormente a fin de garantizar un procesamiento y almacenamiento adecuados.

Asimismo, informará las necesidades detectadas para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento y puedan planificar una adecuada acción correctiva.

4.4.6.3 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. Asimismo verificará el uso de antivirus en las computadoras el cual contará con su respectiva licencia.

- En todos los equipos, tanto de las estaciones de trabajo como de los servidores de la empresa, deberá existir una herramienta antivirus ejecutándose permanentemente y en continua actualización.
- Asimismo está prohibido el uso de usb y discos compactos provenientes de otra fuente que no sea de la empresa.

- Todos los archivos adjuntos recibidos a través del correo electrónico desde Internet deben ser revisados por un antivirus antes de ejecutarlos.
- Deberá existir un procedimiento formal a seguir en caso que se detecte un virus en algún equipo del sistema.
- En caso de infección el área de seguridad informática deberá hallar el origen de la infección por virus informático, para evitar la reinfección de los demás equipos de la empresa.

4.4.6.4 MANTENIMIENTO

4.4.6.4.1 Resguardo de la Información

El Responsable del Área Informática y el de Seguridad Informática junto a los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad.

En base a ello, se definirá y documentará un esquema de resguardo de la información.

4.4.6.4.2 Registro de Actividades del Personal Operativo

El Responsable del Área Informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

a) Tiempos de inicio y cierre del sistema.

b) Errores del sistema y medidas correctivas tomadas.

c) Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.

d) Ejecución de operaciones críticas

e) Cambios a información crítica

4.4.6.4.3 Registro de Fallas

El Responsable del Área Informática desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

4.4.6.5 ADMINISTRACIÓN DE LA RED

El Responsable de Seguridad Informática definirá e implementará controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la empresa, contra el acceso no autorizado.

- El cableado debe seguir las normas del cableado estructurado, que garantizan el funcionamiento eficiente de la red.
- Se deberá asegurar la integridad, exactitud, disponibilidad y confidencialidad de los datos transmitidos, ya sea a través de

los dispositivos de hardware, de los protocolos de transmisión, o de los controles aplicativos.

- Deberá contar con documentación (planos) que describan la ubicación de nodos y recorrido del cableado de la red, para un mantenimiento eficiente del cableado en caso de ocurrir fallas del mismo.
- Deberán existir medios alternativos de transmisión en caso de que alguna contingencia afecte al medio primario de comunicación.
- Deberá medirse periódicamente el nivel de interferencia que existe en la red. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.
- Deberá medirse periódicamente nivel de ancho de banda de red ocupado. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.
- Ante un corte del suministro de energía eléctrica debe apagarse los equipos del centro de cómputo de forma segura, como medida de prevención.

4.4.6.6 ADMINISTRACIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO

El responsable de seguridad informática, implementará procedimientos para la administración de medios informáticos removibles, como discos, usb e informes impresos.

deben mantener las copias generadas, siendo conveniente su encriptación.

- Trimestralmente deberán efectuarse pruebas para probar la capacidad de restaurar información en caso sea necesario. Estas pruebas deben efectuarse en un ambiente distinto al ambiente de Desarrollo de Sistemas.
- El medio que contenga los backup o copias de respaldo deberán ser enviadas a un local remoto periódicamente, de acuerdo a lo establecido por el área de sistemas.
- No deberán utilizarse los **servidores** de la empresa como medios de almacenamiento de las copias de respaldo de ningún sistema.
- Se deberá generar una copia de respaldo de toda la documentación del centro de cómputo, incluyendo el hardware, el software, la cual deberá ser de acceso restringido y estar físicamente en un lugar distinto a los centros de procesamiento.
- Los algoritmos de encriptación son técnicas aceptables para las necesidades de los negocios de hoy. Estas pueden ser empleadas para satisfacer los requerimientos de encriptación de datos de la empresa. La encriptación de datos ofrece protección ante accesos no autorizados a la misma.

4.4.7 CONTROL DE ACCESOS

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

4.4.7.1 Registro de Usuarios

El Responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario.

- Cada usuario de un sistema automatizado debe identificarse de manera única, y su acceso y actividad en los sistemas debe ser controlado, monitoreado y revisado.
- Las terminales deben bloquearse luego de quince (15) minutos de inactividad. El usuario tendrá que autenticarse antes de reanudar su actividad.
- El usuario debe ser instruído en el uso correcto de las características de seguridad del terminal y funciones de todas las plataformas, estaciones de trabajo, etc. y debe cerrar la sesión o bloquear la estación de trabajo cuando se encuentre desatendida o se retire momentáneamente.
- El área de Recursos Humanos deberá comunicar inmediatamente al área de Informática los cambios del personal que se produzcan o el despido de algún empleado, señalando en la comunicación se debe indicar el nombre, la

- El área de Recursos Humanos deberá comunicar inmediatamente al área de Informática los cambios del personal que se produzcan o el despido de algún empleado, señalando en la comunicación se debe indicar el nombre, la fecha efectiva de la baja, su clasificación y cualquier medida o control especial que sea necesario realizar.
- Se debe llevar a cabo una política de desvinculación del personal, a través del cual se quitan permisos al empleado en cuanto a los accesos a los sistemas, cuando un empleado es despedido, evitando un posible acto de venganza por insatisfacción con la decisión de la Empresa.
- El área de Informática se encargará de la generación de cuentas de usuario en los sistemas así como la asignación de perfiles y contraseñas correspondientes, para luego entregarlas al usuario final, con la confidencialidad requerida.
- Los administradores de los sistemas deben realizar monitoreo periódico de los sistemas como parte de su rutina diaria de trabajo, este monitoreo no debe estar limitado solamente a la utilización y performance del sistema sino debe incluir el monitoreo del acceso de los usuarios a los sistemas.
- Se deberían utilizar limitaciones en el tiempo de conexión tanto para estaciones de trabajo como servidores (horario de trabajo) y así proporcionar un nivel de seguridad adicional a las aplicaciones informáticas. Si un usuario no autorizado

área de Informática quien brindará la ampliación del horario para esa cuenta.

4.4.7.2 Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

- Se debe otorgar a los usuarios acceso solamente a la información mínima necesaria para la realización de sus labores.
- Esta tarea puede ser realizada utilizando una combinación de: Seguridad lógica de aplicación, ocultar opciones no autorizadas en los sistemas, limitar los permisos a los archivos de los sistemas (solo lectura), controles sobre la información de salida de los sistemas (reportes, etc.).

4.4.7.3 Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal.

- Todas las contraseñas deben expirar dentro de 90 días. Es recomendable no sea menos de (30) días.
- No debe permitirse la reutilización de ninguna de las 5 últimas contraseñas. Esto asegura que los usuarios no utilicen las mismas contraseñas en intervalos regulares.
- Todos los sistemas deben estar configurados para deshabilitar los identificadores de los usuarios en caso de ocurrir (3) intentos fallidos de autenticación.
- Todas las contraseñas deben tener una longitud mínima de ocho (8) caracteres alfanuméricos y no deben contener espacios en blanco.
- Las contraseñas deberán ser una combinación entre caracteres y letras para ser más difíciles de adivinar.
- En los casos que los sistemas utilizados no soporten controles para las características establecidas para la estructura, vigencia, reutilización e intentos fallidos de ingreso, se debe documentar la excepción a la política, detallando la viabilidad de modificar la aplicación para soportar las características establecidas para las contraseñas.
- Es importante que todos los empleados protejan sus contraseñas, debiéndose seguir las siguientes regulaciones: Bajo ninguna circunstancia, se debe escribir las contraseñas en papel, o almacenarlas en medios digitales no encriptados;

las contraseñas no deben ser divulgadas a ningún otro usuario, si esto ocurriera el área de Informática deberá encargarse de cambiarla durante el próximo ingreso; el usuario autorizado es responsable de todas las acciones realizadas por alguna persona a quien se le ha comunicado; los sistemas no deben mostrar la contraseña en pantalla o en impresiones, para prevenir que éstas sean observadas o recuperadas.

4.4.8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

4.4.8.1 APLICACIONES EN PC'S

- Deberá existir un procedimiento donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.
- El encargado informático estará a cargo de la instalación y la actualización de las aplicaciones. Asimismo realizará chequeos periódicos a fin de verificar instalación de software no autorizado.
- Antes de hacer un cambio en la configuración de los servidores se deberá hacer un backup de la configuración existente. Una vez que el cambio ha resultado satisfactorio deberá almacenarse la configuración modificada.

- Se deberá establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores en el caso de generarse problemas.
- Se deberán documentar no sólo el procedimiento de instalación y reparación y/o mantenimiento de equipos que se realicen.
- Capacitación a los usuarios en el uso de los sistemas, de parte de personal informático responsable.

4.4.8.2 BASE DE DATOS :

- Todos los archivos, las carpetas donde se encuentran almacenados las BD y las aplicaciones de la empresa deberán tener controles de acceso, de manera que solo el responsable de informática sea quien lo administre.

  Se deberán registrar las siguientes ocurrencias:

  - Tiempo y duración de los usuarios en el sistema.
  - Número de conexiones a bases de datos.
  - Número de intentos fallidos de conexiones a bases de datos.
  - Estadísticas de entrada-salida para cada usuario.
  - Generación de nuevos objetos de bases de datos.
  - Modificación de datos.

- Deberán hacerse chequeos regulares de la seguridad de la base de datos, en los que se deberá verificar que:

  ✓ Se hacen y son efectivos los backups y los mecanismos de seguridad.

- ✓ No haya usuarios de la base de datos que no tengan asignado una contraseña.
- ✓ Se revisen los perfiles de los usuarios que no han usado la base de datos por un período largo de tiempo, o solo el administrador de datos tiene acceso de lectura y escritura en los archivos de programa, o la base de datos y las aplicaciones que la administran tiene suficientes recursos libres para trabajar eficientemente.

- Deben mantenerse registros de todas las transacciones realizadas en la base de datos, de manera que éstas puedan revertirse en caso de surgir un problema.

4.4.8.3 SOFTWARE

El sistema operativo de los servidores deberá presentar las siguientes características:

- Alta confiabilidad.
- Compatibilidad e interoperabilidad con los sistemas operativos de las PC´S.
- Escalabilidad.
- Disponibilidad de software de aplicación y actualizaciones,
- Buena administración y generación de logs.
- Buena performance,
- Equilibrio en costo y beneficio.
- Amigable con el usuario.

Todos los programas instalados en las computadoras deben tener licencia, ser aprobados y periódicamente inventariados.

4.4.8.4 CICLO DE VIDA

*Deberá utilizarse un **Plan de Desarrollo de Sistemas**, donde se definan las asignaciones de recursos, el establecimiento de prioridades y responsabilidades de los sistemas informáticos a desarrollarse.

*La empresa deberá contar con personal específicamente para el desarrollo de sistemas que esta necesitara.

*Se deberá implementar una gestión de configuración, y deberán documentarse los cambios desarrollados en las aplicaciones.

*Deberá existir un documento formal de solicitud de cambios (formulario), donde quede reflejado el motivo y la solicitud del cambio, allí se agregarán los requerimientos de seguridad necesarios, definidos por el responsable de la información y el administrador de sistemas. La documentación de los cambios debe incluir:

- Sistema que afecta.
- Fecha de la modificación.
- Desarrollador que realizó el cambio.
- Empleado que solicitó el cambio.
- Descripción global de la modificación.

*El formulario anterior se utilizará para actualizar la documentación del desarrollo y de los distintos manuales generados.

*Deberán realizarse pruebas del software desarrollado, para esto se generarán planes y escenarios de prueba y se documentarán los resultados.

*Los procedimientos de prueba deben estar documentados en los formularios de solicitud de cambio. Si se notara problemas durante el proceso de prueba, el usuario deberá documentar el problema, el desarrollador de sistemas debe realizar las modificaciones apropiadas en el ambiente de desarrollo y entregar al área usuaria para que se vuelva a aprobar.

*La metodología para el desarrollo y mantenimiento de sistemas debe contemplar una revisión de post-implantación del sistema en operación, que deberá determinar si se han logrado los objetivos previstos, y si se ha alcanzado la satisfacción de las necesidades planteadas por los usuarios.

*Todas las modificaciones significativas, mejoras grandes y sistemas nuevos deben ser probados y aprobados por los usuarios del sistema antes de la instalación del software en el ambiente de trabajo.

*Durante las pruebas de aceptación, restricciones lógicas de acceso deben asegurar que los desarrolladores no tengan acceso de actualización y que el código fuente siendo probado no pueda ser

modificado sin consentimiento escrito por el usuario. Si se notara problemas, el usuario debe documentar el problema, el desarrollador debe realizar las modificaciones apropiadas en el ambiente de desarrollo y lo entregará para volver a probarlo.

*Se deberá informar por escrito la importancia de la seguridad de la información a todo el personal contratado. El administrador del área de sistemas, junto con los directivos, serán quienes:

- Especifiquen los requerimientos de seguridad.
- Determinen los pasos a seguir en caso que no se respete lo establecido en el contrato.

*Establezcan cláusulas sobre confidencialidad de la información.

4.4.8.5 DOCUMENTACIÓN :

Se debe incluir estándares para la documentación de las aplicaciones y las actividades. Esta documentación deberá mantenerse actualizada y abarcar todas las fases del ciclo de vida del desarrollo de los sistemas.

Se deberá elaborar y documentar los manuales de usuarios de los sistemas informáticos y mantenerlos actualizados.

4.4.9 GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

- Se deberá contar con un plan de contingencias, el cual será debidamente actualizado; el cual abarcará las diferentes áreas de riesgo.

- Se deberá prever un programa de entrenamiento para el personal involucrado en el plan de contingencias.

- Se deberá asignar un *orden de importancia* a los sistemas de información y a los equipos de la red informática, de acuerdo al análisis de riesgo y al impacto que representaría para la empresa su ausencia.

- Los equipos deberán estar señalizados o etiquetados de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.

- Deberán definirse las funciones o servicios críticos de la empresa, junto con los recursos mínimos necesarios para su funcionamiento, asignándoles una prioridad en el plan de contingencia.

- Debe definirse hasta cuanto tiempo se aceptará estar en condición de emergencia.

- Se deberá almacenar una copia del plan de contingencias en el exterior de la empresa.

- Debe documentarse la realización de las siguientes actividades después de un incidente:

a) Deberá estar documentado antes de su puesta en práctica.

b) Determinar la causa del daño.

c) Evaluar la magnitud del daño que se ha producido.

d) Que sistemas se han afectado.

e) Qué modificaciones de emergencia se han realizado.

f) Que equipos han quedado no operativos.

g) cuales se pueden recuperar y en cuanto tiempo.

Cada una estas actividades deberán ser reportadas por los líderes de cada área a un miembro de la Gerencia.

- Se deberán realizar simulacros de siniestros para evaluar la eficacia y eficiencia del plan.

4.4.10 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

El responsable de seguridad informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia. En la empresa además se tendrán en cuenta los siguientes puntos para asegurar la continuidad del negocio:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la empresa.

- Evaluar los riesgos para determinar el impacto de dichas interrupciones.

- Identificar los controles preventivos.

- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la empresa.

- Elaborar un plan de continuidad necesario para garantizar el desarrollo normal de las actividades de la empresa.

4.4.11 CONFORMIDAD

Toda ley, norma, regulación o acuerdo contractual debe ser documentado y revisado por el Área Legal de la empresa o en caso contrario consultar un profesional en la materia. Requerimientos específicos para controles y otras actividades relacionadas a estas regulaciones legales deben ser delegados al área organizacional respectiva, la cual es responsable para el cumplimiento de la norma en cuestión.

Los recursos informáticos de la empresa deben ser empleados exclusivamente para tareas vinculadas al negocio.

4.4.11.1 Revisión de la Política de Seguridad y Cumplimiento Técnico:

El gerente y jefe de áreas deben asegurarse que las responsabilidades de seguridad sean cumplidas y las funciones relacionadas se ejecuten apropiadamente.

Es responsabilidad del personal encargado de la administración de la seguridad verificar el cumplimiento de las políticas de seguridad. Las excepciones deben ser reportadas a la gerencia apropiada.

4.4.11.2 Propiedad de los Programas :

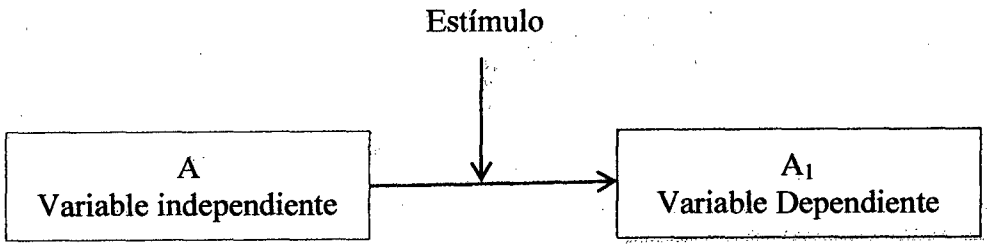
Cada programa elaborado por los desarrolladores de la empresa, debe contener la información de derecho de autor correspondiente. Generalmente, el aviso debe aparecer cuando el usuario inicie la aplicación. Un aviso legible también debe estar anexado a las copias de los programas almacenados en dispositivos como CDs, DVD's .

CAPÍTULO V

DISCUSIÓN

5. 1 CONTRASTACIÓN

Para efectos de la contrastación de la hipótesis propuesta en la presente investigación se utilizó el modelo de sucesión en línea:



Donde:

A : Plan de Seguridad Informático

A_1 : Mejora en la calidad en el servicio del call center

Estímulo: Aumento en la cantidad de ventas por teleoperador, reducción de llamadas perdidas por falla de red y reducción de quejas por falla en la red.

A través de esto se evaluó la variable dependiente, en este caso mejorar la calidad del servicio del call center, en base a los efectos de la aplicación de la variable independiente, que está representada por la implementación del plan de Seguridad Informático.

Para ello la evaluación de los efectos en la variable dependiente con respecto a la variable independiente, usamos tres indicadores como son:

- Cantidad de ventas por Teleoperador
- Cantidad de llamadas perdidas por falla en la red informática
- Cantidad de fallas por falla en la red informática

• Cantidad de fallas por falla en la red informática

A continuación se muestran los resultados de la evaluación de los indicadores basados en el plan de Seguridad Informático.

INDICADOR / MES	VENTAS	
	Antes de la aplicación del Plan de Seguridad Informático (Año 2011)	Después de la aplicación del Plan de Seguridad Informático (Año 2012)
Enero	82	105
Febrero	98	184
Marzo	104	186
Abril	100	182
Mayo	120	214
Junio	103	247
Julio	95	231
Agosto	109	267
Setiembre	88	290
Octubre	95	266
Noviembre	105	298
Diciembre	101	305
TOTAL	**1200**	**2775**
PROMEDIO	**100**	**231.25**

Tabla N° 32: Cantidad de Ventas Por Teleoperador

Fuente: Datos tomados en campo

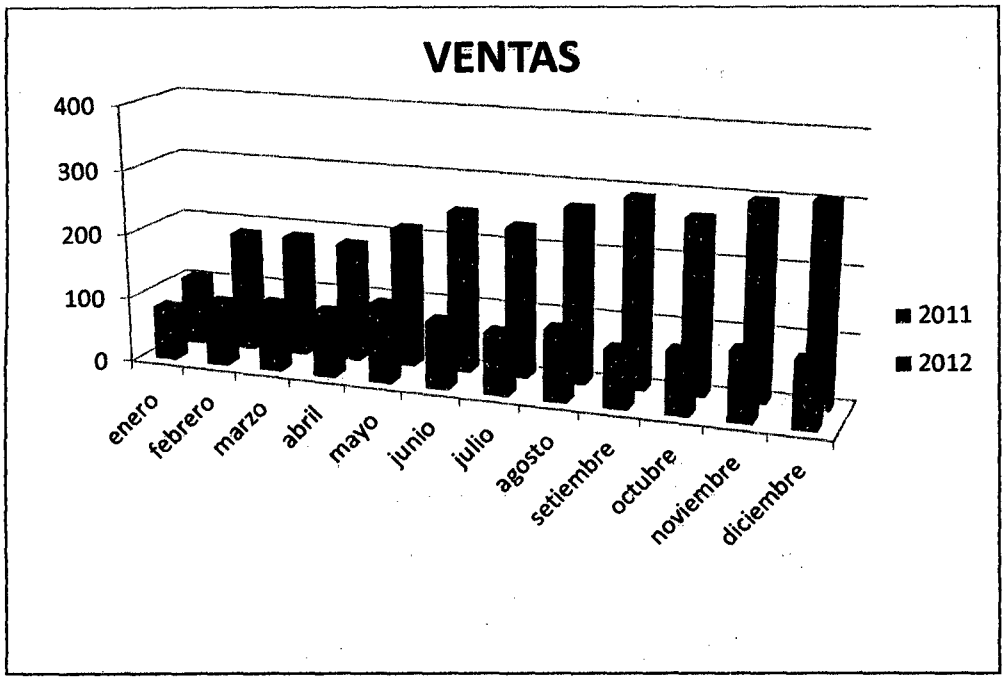


Gráfico N° 12: Gráfica comparativa de Ventas anuales

Interpretación:

El resultado obtenido luego de las pruebas realizadas, nos permite apreciar que existe una mayor cantidad de ventas por teleoperador después de aplicar la implementación del plan de seguridad informático lo que nos indica que existe una gran ventaja respecto a las ventas antes de aplicar el plan de seguridad Informático.

INDICADOR / MES	LLAMADAS PERDIDAS	
	Antes de la aplicación del Plan de Seguridad Informático (Año 2011)	Después de la aplicación del Plan de Seguridad Informático (Año 2012)
Enero	9	5
Febrero	9	6
Marzo	8	6
Abril	10	5
Mayo	9	4
Junio	11	3
Julio	10	3
Agosto	8	3
Setiembre	12	5
Octubre	12	4
Noviembre	11	2
Diciembre	10	2
TOTAL	119	48
PROMEDIO	9.916666667	4

Tabla N° 33: Cantidad de llamadas perdidas por falla en la red informática

Fuente: Datos tomados en campo

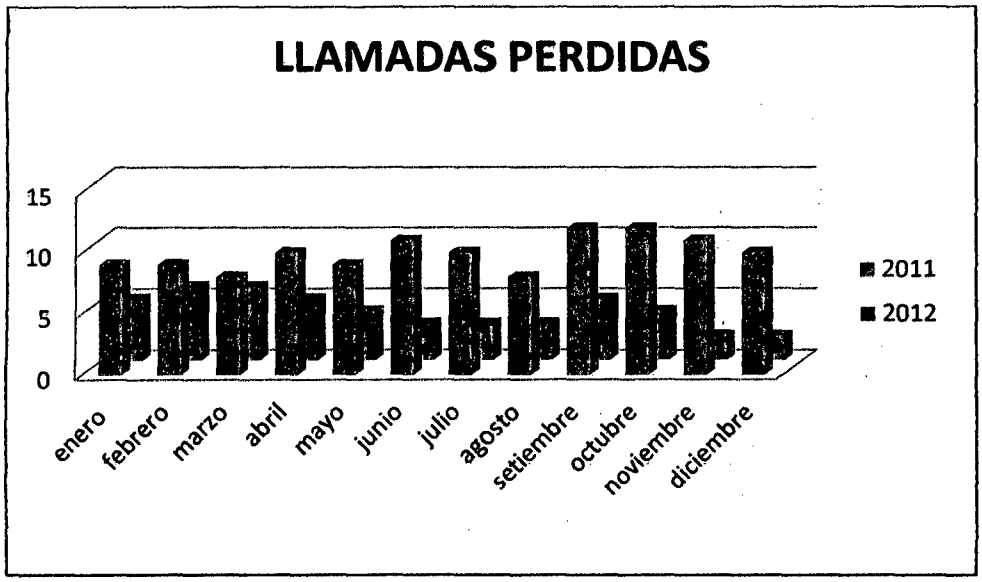


Gráfico N° 13: Gráfica comparativa de Llamadas Perdidas anuales

Interpretación:

El resultado obtenido luego de las pruebas realizadas, nos permite apreciar que existe una menor cantidad de llamadas perdidas por falla en la red informática después de la aplicación del plan de seguridad informático.

INDICADOR / MES	QUEJAS	
	Antes de la aplicación del Plan de Seguridad Informático (Año 2011)	Después de la aplicación del Plan de Seguridad Informático (Año 2012)
Enero	9	6
Febrero	6	6
Marzo	11	5
Abril	9	4
Mayo	10	5
Junio	11	3
Julio	13	3
Agosto	12	3
Setiembre	10	3
Octubre	11	2
Noviembre	12	2
Diciembre	15	2
TOTAL	129	44
PROMEDIO	10.75	3.666666667

Tabla N° 34: Cantidad de quejas por falla en la red informática

Fuente: Datos tomados en campo

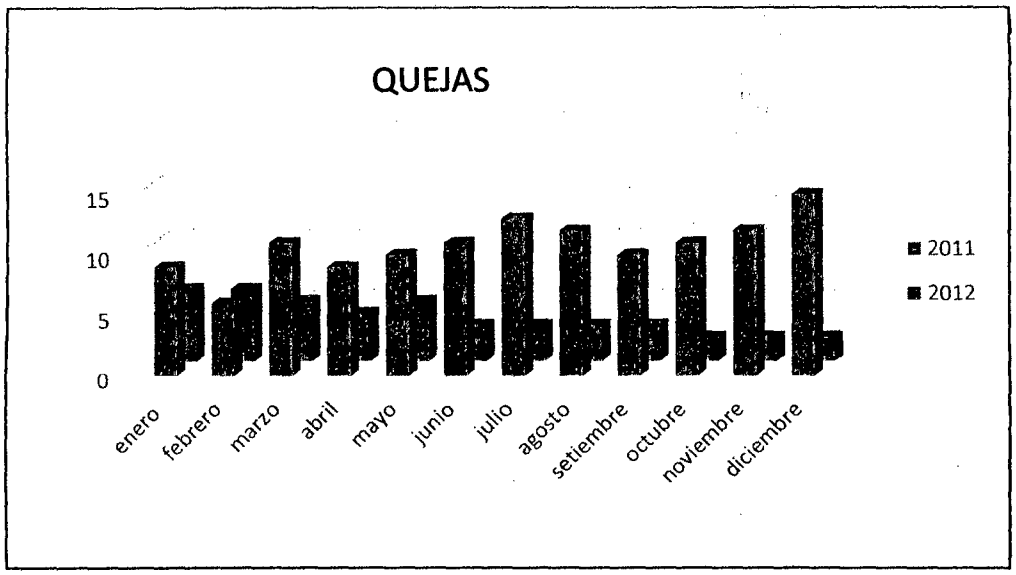


Gráfico N° 14: Gráfica comparativa de Quejas por falla en la red anuales

Interpretación:

El resultado obtenido luego de las pruebas realizadas, nos permite apreciar que existe una menor cantidad de quejas por falla en la red informática después de la aplicación del plan de seguridad informático.

CONCLUSIÓN

Por el resultado de los tres indicadores de evaluación, se puede determinar que la implementación de un Plan de Seguridad Informático mejora la calidad en el servicio del call center de la empresa TELSAT PERÚ SAC.

CONCLUSIONES

- Se propuso un Plan de Seguridad Informático, el cual permitió mejorar la calidad del servicio que brinda el call center de la empresa Telsat Perú SAC, aumentando las ventas en un 231.25%, disminuyendo las quejas en un 34.11%, las llamadas perdidas por falla en la red se redujeron en un 40.34%.
- Se realizó un análisis del estado en que se encontró la red informática de la empresa, detectándose fallas en la red informática y pérdidas de llamadas, determinando así los activos que tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos.
- Se identificaron las 11 secciones referidas a la seguridad informática a fin ser evaluadas y luego proponer controles que mejoren la Seguridad informática en la empresa Telsat Perú SAC.
- El Plan de Seguridad Informático propuesto, establece los mecanismos y requerimientos mínimos establecidos en los estándares desarrollados por los entes reguladores como el estándar de seguridad de información ISO /IEC 27002.
- Se implementó el Plan de Seguridad Informático en un 80% lo cual permitió definir las políticas de Seguridad Informática en la empresa, de esta manera asegurar la confidencialidad, integridad y disponibilidad de la información.

RECOMENDACIONES

- Capacitar y concientizar al personal sobre el cumplimiento constante de las políticas de seguridad que se mencionan en el Plan de Seguridad informático propuesto.
- Se recomienda la creación de un Comité de Seguridad Informática, que se encargue de la administración de seguridad de la información, y que controle la protección de los activos informáticos de la organización tanto físicos (instalaciones, hardware) como lógicos (software, datos), promueva la seguridad en la empresa por medio de un compromiso apropiado y de los recursos adecuados, que asegure una dirección con iniciativas de seguridad.
- Permitir a los usuarios conocer las necesidades de toda la empresa (no sólo las de su área) y participar en la fijación de prioridades, realizar el monitoreo y evaluación del desarrollo de la actividad informática interna y el cumplimiento de las políticas y normas dictadas en la materia; así como promover el aprovechamiento de nuevas tecnologías y fomentar la adecuada capacitación de los servidores; es decir velar por el desarrollo informático en toda la empresa.
- El área de Informática debe tener en cuenta siempre la realización de backups de información previa periodicidad de la misma, asegurar su almacenamiento adecuado y disponibilidad cuando se presenten contingencias.
- Invertir en tecnología, nuevos equipos para monitorear y resguardar la seguridad de los equipos de cómputo del call center; así también brindar mayor seguridad y control a la información asegurando su confidencialidad, integridad y disponibilidad.

- *Lacayo Arzú, A. (2004). Análisis e Implementación de un esquema de Seguridad en Redes para la Universidad de Colima.* (Tesis de maestría, Universidad de Colima), Recuperado de http://digeset.ucol.mx/tesis_posgrado/Pdf/Aaron_Clemente_Lacayo_A.pdf
- Laudon, K. & Laudon, J. (1995). *Administración de los Sistemas de Información.* México: Editorial Mc Graw – Hill Interamericana de México S.A.
- Martínez, J. (2009). Seguridad Informática. Recuperado el 01 de julio de 2011, de http://www.antoniomtz.org.
- Metodología para la elaboración del Plan de Seguridad Informática(s.f.). Revisado el 15/12/2011, de http://files.sld.cu/gau/files/2009/03/plan_seguridad.pdf.
- Piattini, M. & del Peso, E. (1998). *Auditoría Informática un Enfoque Práctico.* España: Alfaomega Grupo Editor S.A.
- Políticas de Seguridad Informática (2005). Recuperado el 16/09/2011, de http://www.monografias.com/trabajos12/fichagr/fichagr.shtml
- Seguridad Informática (s.f.). Recuperado el 22/08/2011, de http://www.monografias.com/trabajos16/seguridadnformatica/seguridad-informatica.shtml

ANEXOS

Diagnóstico de la empresa

Como ayuda a la realización del análisis de requisitos se ha realizado dentro de la empresa el cuestionario de diagnóstico basado en la norma ISO/IEC 27002.

ANEXO N° 1

"EVALUACIÓN DE LA POLÍTICA DE SEGURIDAD"

1. ¿Se ha definido una política de seguridad de información?

   Si ( ) No (*)

2. ¿De haberse definido una política de seguridad de la información, se están aplicando las políticas de seguridad de la información?

   Si ( ) No (*)

3. ¿Se hace de conocimiento al personal de la empresa las políticas de seguridad de la información?

   Si ( ) No (*)

4. ¿Existe normativa y procedimientos relativos a la seguridad de los S.I.?

   Si ( ) No (*)

5. ¿Se realizan evaluaciones y actualizaciones constantes, en caso las haya, de las políticas de seguridad de la información?

   Si ( ) No (*)

6. ¿Las políticas de seguridad de la información, si en caso las tuvieran, están basadas en algún estándar nacional o internacional?

   Si ( ) No (*)

7. ¿Existe un responsable de las políticas, normas y procedimiento?

   Si ( ) No (*)

ANEXO N° 2

"EVALUACIÓN DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN"

1. ¿La empresa tiene un Comité informático que se encargue de la Seguridad de la información a nivel de la alta dirección?

   Si ( ) No (*)

2. ¿El área de Informática se encuentra ubicado en la estructura organizativa general de la empresa? ¿Cuenta con autoridad para disponer independencia frente a las demás áreas?

   Si (*) No ( )

3. ¿Los usuarios participan en el Comité, para determinar los requerimientos de la información de las áreas y así determinar las prioridades de los proyectos?

   Si ( ) No (*)

4. ¿Las descripciones de las funciones, responsabilidades del área de Informática están documentadas y son actuales? ¿Existe una adecuada segregación de funciones, incluyendo la separación entre desarrollo de sistemas de información, soporte, áreas usuarios?

   Si ( ) No (*)

5. ¿Se ha elaborado un Plan Operativo del área de sistemas?

   Si ( ) No (*)

6. ¿Se ha elaborado un Plan Estratégico de Sistemas de Información; se encuentra debidamente documentado y aprobado por el Comité de Informática? ¿Los objetivos del Plan Estratégico están alineados con los objetivos de la Empresa?

   Si ( ) No (*)

7. ¿Tiene la empresa un área o una persona asignada para labores exclusivas de seguridad de la información?

   Si ( ) No (*)

8. ¿Existe un responsable encargado de evaluar la adquisición y cambios de los Sistemas Informáticos?

   Si (*) No ( )

ANEXO N° 3

"EVALUACIÓN DE LA GESTION DE ACTIVOS

1. ¿Existe un inventario actualizado de los activos informáticos de la Empresa?

   Si ( ) No (*)

2. ¿El inventario contiene activos de datos, software, equipos y servicios?

   Si ( ) No (*)

3. ¿Realizan periódicamente la actualización de su inventario de los activos informáticos?

   Si ( ) No (*)

4. ¿Se dispone de una clasificación de los activos de información de acuerdo a la importancia de los mismos?

   Si ( ) No (*)

5. ¿Existen procedimientos para clasificar la información?

   Si ( ) No (*)

ANEXO N° 4

"EVALUACIÓN DE LA SEGURIDAD LIGADA A LOS RR.HH."

1. ¿Se tienen definidas responsabilidades y roles de seguridad?

   Si ( ) No (*)

2. ¿Se tiene en cuenta la seguridad en la selección de personal?

   Si ( ) No (*)

3. ¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?

   Si ( ) No (*)

4. ¿Reciben los usuarios capacitación actualizada en temas de seguridad de la información?

   Si ( ) No (*)

5. ¿Se identifican los usuarios para poder ingresar a la empresa?

   Si (*) No ( )

6. ¿Existe algún procedimiento a seguir en caso de algún incidente de seguridad?

   Si ( ) No (*)

7. ¿Se recogen los datos de los incidentes de forma detallada?

   Si ( ) No (*)

8. ¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?

   Si (*) No ( )

9. ¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?

   Si (*) No ( )

ANEXO N° 5

"EVALUACIÓN DE LA SEGURIDAD FÍSICA Y DEL ENTORNO"

1. ¿Existe un perímetro de seguridad física?

   Si (*) No ( )

2. ¿Existe un adecuado control en el acceso físico en el área de informática?

   Si ( ) No (*)

3. ¿El área de informática tiene una oficina independiente de las demás áreas de la empresa?

   Si ( ) No (*)

4. ¿Se mantiene un registro de todas las personas que ingresan y salen del área de informática o de la empresa?

   Si ( ) No (*)

5. Se apagan los servidores en algún momento; es necesario que queden prendidos las 24 horas?

   Si (*) No ( )

6. ¿Las computadoras tienen deshabilitados los dispositivos externos, como la lectora de CD?

   Si ( ) No (*)

7. ¿La BIOS tiene habilitada una contraseña? ¿Cómo se controla este dispositivo?

   Si ( ) No (*)

8. ¿Cuentan un plan de mantenimiento preventivo o correctivo tanto para hardware como software en los equipos informáticos?

   Si ( ) No (*)

9. ¿Existe un control sobre los dispositivos que se instalan en las computadoras?

   Si ( ) No (*)

10. ¿Existen protecciones frente a fallos en la alimentación eléctrica?

    Si ( ) No (*)

11. ¿Existen extintores ante posibles incendios?

    Si (*) No ( )

12. ¿Se cuenta con un Sistema de aire acondicionado?

    Si ( ) No (*)

13. ¿Existen planos descriptivos de los puntos de red?

    Si ( ) No (*)

14. ¿Existe vigilancia en el departamento de cómputo las 24 horas?

    Si ( ) No (*)

15. ¿Existen políticas de limpieza en el puesto de trabajo?

    Si (*) No ( )

ANEXO N° 6

"EVALUACIÓN DE LA GESTIÓN DE COMUNICACIONES Y OPERACIONES"

1. ¿Cuentan con procedimientos y responsabilidades operativas y documentadas del uso y acceso a los sistemas informáticos?

   Si ( ) No (*)

2. ¿Existe un control para el acceso a Internet?

   Si (*) No ( )

3. ¿Existen carpetas compartidas en las computadoras de la red?

   Si (*) No ( )

4. ¿Se cuentan con licencias de antivirus para todos los equipos existentes?

   Si ( ) No (*)

5. ¿Tienen procedimientos formales a seguir en caso de infección de virus?

   Si ( ) No (*)

6. ¿Se cuentan con licencias correspondientes del software instalado?

   Si ( ) No (*)

7. ¿Se realizan copias de seguridad de los archivos, datos y programas de los sistemas de información?

   Si (*) No ( )

8. ¿Tienen un control documentado de las direcciones IP de las máquinas de los usuarios y de los planos descriptivos de los puntos de la red informática?

   Si ( ) No (*)

ANEXO N° 7

"EVALUACIÓN DEL CONTROL DE ACCESOS"

1. ¿Se ha definido el nivel de acceso a los usuarios? Es decir, a qué recursos tienen acceso y a qué recursos no?

   Si (*) No ( )

2. ¿Los usuarios del sistema tienen asignado una fecha de expiración del password.?

   Si ( ) No (*)

3. ¿Es bloqueado el sistema cuando un usuario digita mal la contraseña de ingreso al sistema?

   Si ( ) No (*)

4. ¿Existe un procedimiento formal para efectuar las bajas de los empleados de los sistemas?

   Si ( ) No (*)

5. ¿Se tiene en cuenta alguna restricción horaria en el momento de permitir a un usuario el logeo al sistema?

   Si ( ) No (*)

6. ¿El sistema ejecuta alguna acción cuando el usuario permanece un largo período de tiempo sin actividad?

   Si (*) No ( )

7. ¿Los servidores permanecen logeados durante las 24 horas del día?

   Si ( ) No (*)

8. ¿Los passwords tienen una longitud mínima requerida por el sistema?

   Si ( ) No (*)

ANEXO N° 8

"EVALUACIÓN DE LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS INFORMÁTICOS"

1. ¿Se cuenta con el total de licencias respectivas del sistema operativo de redes y de todas las computadoras, se mantienen actualizado el sistema operativo?
   Si ( ) No (*)
2. ¿Se realizan controles de acceso lógico a la base de datos y a los programas fuente de las aplicaciones que se utiliza en la red de la empresa?
   Si ( ) No (*)
3. ¿La información tiene asignado un responsable conforme a su clasificación?
   Si ( ) No (*)
4. ¿Existe un adecuado modelamiento de la base de datos por parte del personal del área de sistemas?
   Si ( ) No (*)
5. ¿Tienen estándares definidos, procedimientos a seguir y documentación respecto a la instalación y actualización de la Configuración de las computadoras?
   Si ( ) No (*)
6. ¿Los usuarios tienen restricciones con respecto a la instalación de programas en sus respectivos puestos de trabajo?
   Si (*) No ( )
7. ¿Conocen los usuarios de los sistemas, las funcionalidades al detalle del mismo?
   Si (*) No ( )
8. ¿Existe un plan de desarrollo de sistemas formal durante el ciclo de vida del software?
   Si ( ) No (*)
9. ¿Existe una gestión de configuración o un control de versiones durante el desarrollo.
   Si ( ) No (*)
10. ¿Existe documentación referente a los sistemas en operación, se actualiza?
    Si ( ) No (*)
11. ¿Tienen manuales de usuario de los sistemas en operación?
    Si ( ) No (*)

ANEXO N° 9

"EVALUACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN"

1. ¿Tienen elaborado planes de contingencia o continuidad de las operaciones informáticas?
   Si ( ) No (*)

2. ¿Están implementadas los planes de continuidad de las operaciones informáticas?
   Si ( ) No (*)

3. ¿Realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones informáticas?
   Si ( ) No (*)

ANEXO N° 10

"EVALUACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO"

1. ¿Existen procesos para la gestión de la continuidad?

   Si ( ) No (*)

2. ¿Existe un plan de continuidad del negocio y análisis de impacto?

   Si ( ) No (*)

3. ¿Existe un diseño, redacción e implantación de planes de continuidad?

   Si ( ) No (*)

4. ¿Existe un marco de planificación para la continuidad del negocio?

   Si ( ) No (*)

5. ¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?

   Si ( ) No (*)

ANEXO N° 11

"EVALUACIÓN DE LA CONFORMIDAD"

1. ¿La empresa cuenta con normativa legal respecto a las aplicaciones que utiliza en la empresa y al uso del software licenciado?

   Si ( ) No (*)

2. ¿Existe un responsable definido en la estructura de la empresa encargado de mantener actualizada las normas emitidas por la Oficina Nacional de Gobierno Electrónico?

   Si ( ) No (*)

3. ¿Se tiene en cuenta el cumplimiento con la legislación?

   Si ( ) No (*)

4. ¿Existe una revisión de la política de seguridad y de la conformidad técnica?

   Si ( ) No (*)

5. ¿Existen consideraciones sobre las auditorias de los sistemas?

   Si ( ) No (*)

PRESUPUESTO PROPUESTO PARA COMPRA DE HARDWARE Y SOFTWARE

HARDWARE	CANT	PRECIO UNIT. (S/)	PRECIO TOTAL (S/)
Servidor PowerEdgeT420	3	5,855.00	17 565.00
UPS Centralion Blazer Vista S 1000, 40 min.	33	475.00	15 675.00
Cintas Tape Backup 80 Gb	10	35.00	350.00
Sensor de humo contra incendios	3	28.00	84.00
Equipo de Aire Acondicionado	1	919.00	919.00
Sensores de Movimiento	2	29.00	58.00
Extintores CO_2 de 2 kg	2	100.00	200.00
Grupo Electrógeno	1	5200.00	10 400.00
Cámara de video-vigilancia	2	216.00	432.00
TOTAL			**45 683.00**

SOFTWARE	CANT	PRECIO UNIT. ($)	LICENCIA X UNIDAD ($)	PRECIO TOTAL ($)
Sistema Operativo Windows Server 2003 Estándar Edition en español	3	486.00	270.00	1 296.00
Sistema Operativo Windows XP Professional SP2 Español	33	200.00	75.00	2 675.00
Power Builder v 11.5	1	3,200.00	0.00	3 200.00
SQL	1	1,180.00	0.00	1 180.00
ISA SERVER 2004	1	1,500.00	0.00	1 500.00
Microsoft Office 2010	33	135.00	130.00	4 425.00
Hacker Antivirus	33	40.00		440.00
TOTAL ($)				**14 716.00**
TOTAL (S/)				**39 733.20**

s/ 110 ($ 40) es x 3 pc

tipo de cambio : 1 $ = s/2.70

OTROS	CANTIDAD	PRECIO UNITARIO (S/)	PRECIO TOTAL (S/)
Personal de seguridad	02	900.00	1800.00
Desarrollador de Sistemas de Información / Administrador de Seguridad de Informática	01	3500.00	3500.00
TOTAL			**5 300.00**

COSTO TOTAL

CONSIDERACIONES	COSTO TOTAL (S/)
HARDWARE Y EQUIPOS DE SEGURIDAD	**45 683.00**
SOFTWARE	**39 733.20**
OTROS	**5 300.00**
COSTO TOTAL	**90 716.20**

UNIVERSIDAD NACIONAL DEL SANTA

OFICINA CENTRAL DE INVESTIGACION

"CATÁLOGO DE TRABAJOS DE INVESTIGACIÓN –TIPRO"
Resolución N° 1562-2006-ANR

REGISTRO DEL TRABAJO DE INVESTIGACIÓN
FACULTAD DE INGENIERÍA

I. DATOS GENERALES (PRE GRADO):

- **UNIVERSIDAD:**
  UNIVERSIDAD NACIONAL DEL SANTA
- **ESCUELA O CARRERA PROFESIONAL:**
  E.A.P DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
- **TÍTULO DEL TRABAJO:**
  PLAN DE SEGURIDAD INFORMÁTICO PARA MEJORAR LA CALIDAD EN EL SERVICIO DEL CALL CENTER DE LA EMPRESA TELSAT PERÚ SAC.
- **ÁREA DE INVESTIGACIÓN:**
  PLAN DE SEGURIDAD INFORMÁTICO
- **AUTOR:**
  DNI: 32991391
  APELLIDOS Y NOMBRES:ANGULO CASTILLO ALEXA MADELYN
- **TÍTULO PROFESIONAL A QUE CONDUCE:**
  Tesis para Optar por el Título Profesional de Ingeniero de Sistemas e Informática.
- **AÑO DE APROBACIÓN DE LA SUSTENTACIÓN:**
  2014

II. CONTENIDO DEL RESUMEN

- **PLANTEAMIENTO DEL PROBLEMA**

  Telsat Perú SAC es una empresa que brinda el servicio de venta y configuración de equipos para enlaces inalámbricos, instalación de Internet inalámbrico residencial de banda ancha e instalación de Sistemas de Televigilancia por internet. Asimismo cuenta con un call center, el cual trabaja para empresas extranjeras como Nuera Telecom y Banco Santander ofreciendo su servicio de llamadas telefónicas internacionales y venta de tarjetas de débito respectivamente, esto para estar a la vanguardia de la tecnología y en su afán de brindar un servicio de comunicación de información eficiente y de forma transparente para el personal.

Telsat Perú SAC tiene 9 años en el mercado y cuenta en la actualidad con 30 pc's las cuales funcionan en su totalidad para el call center, el cual utiliza software como: Eyebeam, Spark, Software de Oficina, Antivirus Corporativo y Sistemas Operativos no licenciados, para ello cuenta con los respectivos servidores que dan soporte a las diferentes aplicaciones y servicios.

En el año 2009, año en que se inicia el funcionamiento del call center, su promedio en ventas mensuales era de 150 ventas aproximadamente, teniendo 14 teleoperadores (ventas hechas para la Empresa Nuera Telecom).

En la actualidad, con el mismo número de teleoperadores, su promedio mensual es de 100 ventas aproximadamente, notándose claramente una disminución de los ingresos mensuales de la empresa.

El motivo principal en estos índices es la deserción de los empleados por la insatisfacción del funcionamiento de la red informática lo cual implica: fallas en la transmisión de los datos en la red, pérdida en la fluidez de la comunicación con los clientes, lentitud, saturación e inoperatividad en la red además ante un corte de fluido eléctrico se cortan las conversaciones de una manera intempestiva y al no contar con los equipos necesarios para evitarlo se pierde la comunicación con el cliente y éste muchas veces ya no contesta cuando se le vuelve a llamar disminuyendo la posibilidad de captar un cliente mas.

En cuanto al cableado se puede observar que está expuesto a interferencias como corriente eléctrica ya que no se encuentran protegidos en su totalidad por canaletas y éstas a su vez están deterioradas. Además la red no cuenta con controles de seguridad que protejan la integridad, confidencialidad y disponibilidad de los datos que en ella se transmiten, por lo tanto la empresa tiene una red informática que no cumple las normas o estándares internacionales de seguridad haciendo que esté vulnerable a ataques, intromisiones de personas no autorizadas, desastres naturales, desastres informáticos, etc. lo que ha ocasionado la pérdida de clientes y recursos para la empresa.

Telsat Perú SAC con la finalidad de mejorar el servicio que brinda en su call center está dispuesta a seguir un plan de seguridad Informático.

- **OBJETIVOS**
  - **Objetivo General**

    Proponer un plan de seguridad informático para mejorar la calidad en el servicio del call center de la empresa Telsat Perú SAC.

  - **Objetivos Específicos**
    - Realizar una revisión bibliográfica a cerca de Planes de Seguridad Informáticos.
    - Recopilar y organizar la información necesaria para entender a la empresa.
    - Analizar el estado del software, los equipos informáticos y de telecomunicaciones del centro de cómputo de la empresa Telsat Perú SAC.
    - Analizar los controles de seguridad informáticos en la empresa Telsat Perú SAC de acuerdo a la Norma ISO/IEC 27002.
    - Desarrollar un análisis de riesgos en la empresa Telsat Perú SAC. , con el propósito de determinar cuáles de los activos de la empresa tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos.
    - Definir las políticas de seguridad que conforman el Plan de Seguridad Informático, basados en el estándar de seguridad internacional ISO/IEC 27002, que garantice minimizar los riesgos identificados.
    - Elaborar el Plan de Seguridad Informático para la empresa Telsat Perú SAC.

- **HIPÓTESIS**

  El Plan de Seguridad Informático mejora la calidad en el servicio del call center de la empresa Telsat Perú SAC.

  VARIABLES

  Variable Independiente : Plan de seguridad informático.

  Indicadores:

  - Número de controles de Seguridad aplicados.

Variable Dependiente : Mejorar la calidad en el servicio del call center

Indicadores:

- Número de ventas por mes del teleoperador
- Número de llamadas perdidas por falla en la red
- Número de quejas por falla en la red del teleoperador

- **BREVE REFERENCIA AL MARCO TEÓRICO**

CALL CENTER

También llamados "centros de llamadas", se trata de una oficina donde un grupo de personas específicamente entrenadas se encarga de brindar algún tipo de atención o servicio telefónico, lo cual está determinado por cada empresa.

Los trabajadores de un call center pueden realizar llamadas (para tratar de vender un producto o un servicio, realizar una encuesta, etc.) o recibirlas (para responder las inquietudes de los clientes, tomar pedidos, registrar reclamos). En algunos casos, el call center se especializa en una de las dos tareas (realizar o recibir los llamados) mientras que, en otros, cumplen con ambas funciones.

Es importante destacar que el call center puede ser operado por la propia compañía o tercerizado en una empresa externa. Hay firmas que se dedican a establecer centros de llamadas (con la infraestructura necesaria y el personal entrenado) y comercializan dicha prestación.

El call center cuenta con estaciones de trabajo que incluyen computadoras, teléfonos, auriculares con micrófonos (headsets) conectados a interruptores telefónicos y una o más estaciones de trabajo pertenecientes a los supervisores del sector.

PLAN DE SEGURIDAD INFORMÁTICO

Es la expresión gráfica del Sistema de Seguridad Informático diseñado y constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una entidad y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

Por tanto, el Plan de Seguridad Informático es un documento en el que establecen las políticas, y acciones que permiten garantizar la prestación de servicios y asegurar la información contenida en un sistema computacional, considerando los lineamientos para promover la planeación, el diseño y la implementación de un modelo de seguridad en la Empresa, con el fin de establecer una cultura de la seguridad en la organización, el cual se basa en normas internacionales como por ejemplo ISO /IEC 27002.

El propósito de establecer éste plan es proteger la información y los activos de la organización, tratando de preservar:

a) Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información.

b) su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.

c) su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

ISO/IEC 27002

Anteriormente llamada ISO 17799, es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000 y con el título de Information technology - Security techniques - Code of practice for information security management. Tras un periodo de revisión y actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799 tiene su origen en Archivo: La norma británica British Standard BS 7799-1 que fue publicada por primera vez en 1995.

En España existe la publicación nacional UNE-ISO/IEC 17799 que fue elaborada por el comité técnico AEN/CTN 71 y titulada *Código de buenas prácticas para la Gestión de la Seguridad de la Información* que es una copia idéntica y traducida del Inglés de la Norma

Internacional ISO/IEC 17799:2000. La edición en español equivalente a la revisión ISO/IEC 17799:2005 se estima que esté disponible en la segunda mitad del año 2006.

En Perú la ISO/IEC 17799:2000 es de uso obligatorio en todas las instituciones públicas desde agosto del 2004, cuando el Ing. César Vilchez propuso la norma al entonces Jefe de la ONGEI - PCM, Rafael Parra Erkel, quién aprobó la iniciativa, estandarizando de esta forma los diversos proyectos y metodologías en este campo, respondiendo a la necesidad de seguridad por el uso intensivo de Internet y redes de datos institucionales, la supervisión de su cumplimiento esta a cargo de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI (www.ongei.gob.pe).

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

La versión de 2005 del estándar incluye las siguientes once secciones principales:

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad de negocio
- Conformidad

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar previamente cuantos serán realmente los aplicables y según sus propias necesidades.

- **CONCLUSIONES Y RECOMENDACIONES**

CONCLUSIONES

- Se propuso un Plan de Seguridad Informático, el cual permitió mejorar la calidad del servicio que brinda el call center de la empresa Telsat Perú SAC, aumentando las ventas en un 231.25%, disminuyendo las quejas en un 34.11%, las llamadas perdidas por falla en la red se redujeron en un 40.34%.
- Se realizó un análisis del estado en que se encontró la red informática de la empresa, detectándose fallas en la red informática y pérdidas de llamadas. determinando así los activos que tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos.
- Se identificaron las 11 secciones referidas a la seguridad informática a fin ser evaluadas y luego proponer controles que mejoren la Seguridad informática en la empresa Telsat Perú SAC.
- El Plan de Seguridad Informático propuesto, establece los mecanismos y requerimientos mínimos establecidos en los estándares desarrollados por los entes reguladores como el estándar de seguridad de información ISO /IEC 27002.
- Se implementó el Plan de Seguridad Informático en un 80% lo cual permitió definir las políticas de Seguridad Informática en la empresa, de esta manera asegurar la confidencialidad, integridad y disponibilidad de la información.

RECOMENDACIONES

- Capacitar y concientizar al personal sobre el cumplimiento constante de las políticas de seguridad que se mencionan en el Plan de Seguridad informático propuesto.
- Se recomienda la creación de un Comité de Seguridad Informática, que se encargue de la administración de seguridad de la información, y que controle la protección de los activos informáticos de la organización tanto físicos (instalaciones, hardware) como lógicos (software, datos), promueva la seguridad en la empresa por medio de un compromiso apropiado y de los recursos adecuados, que asegure una dirección clara y el apoyo visible de la gerencia a las iniciativas de seguridad.
- Permitir a los usuarios conocer las necesidades del conjunto de la organización - no sólo las de su área – y participar en la fijación de prioridades, realizar el monitoreo y evaluación del desarrollo de la actividad informática interna y el cumplimiento de las políticas y normas dictadas en la materia; así como promover el aprovechamiento de nuevas tecnologías y fomentar la adecuada capacitación de los servidores en la empresa en el campo de la informática; es decir velar por el desarrollo informático en toda la empresa.
- El área de Informática debe tener en cuenta siempre la realización de backups de información previa periodicidad de la misma, asegurar su almacenamiento adecuado y disponibilidad cuando se presenten contingencias.
- Invertir en tecnología, nuevos equipos para monitorear y resguardar la seguridad de los equipos de cómputo del call center ; asi también brindar mayor seguridad y control a la información asegurando su confidencialidad, integridad y disponibilidad.

BIBLIOGRAFÍA

- Aguirre, Y.(2003). Propuesta de implantación del área de auditoría en informática en un órgano legislativo. Recuperado el 30/08/2011, de http://olea.org/~yuri/propuesta-implantacion-auditoria-informatica-organo-legislativo/ch03s03.html
- Centro de llamadas (s.f.). Recuperado el 19/08/2011, de http://es.wikipedia.org/wiki/Centro_de_llamadas
- Corletti, A. (2006). ISO-27001: Los Controles. Recuperado el 20/08/2011, de http://www.delitosinformaticos.com/11/2006/seguridad-informatica/iso-27001-los-controles-parte-i
- Chacón ,Erazo , España ,Montoya y Portillo (2009). Recuperado el 08/08/2011, de http://www.monografias.com/trabajos67/estandar-internacional/estandar-internacional2.shtml
- Daltabuit, E.; Hernández, L.; Mallén, G. & Vázquez, José. (2007). *La Seguridad de la información*. México: Limusa.
- De Marcelo, J (2002). *Piratas Cibernéticos. Cyberwars, Seguridad Informática e Internet*. Mexico D.F. :Alfaomega Grupo Editor S.A. de C.V.
- Groth, D. & Skandier, T. (2005). Guía del estudio de redes. Recuperado el 19/09/2011, de http://es.wikipedia.org/wiki/Red_de_computadoras
- Implementación y Plan de Seguridad Informática(s.f.) Recuperado el 12/08/2011, de http://www.piramidedigital.com/Documentos/ICT/pdictseguridadinformaticaimplementacion.pdf.
- *Lacayo Arzú, A. (2004). Análisis e Implementación de un esquema de Seguridad en Redes para la Universidad de Colima.* (Tesis de maestría, Universidad de Colima), Recuperado de http://digeset.ucol.mx/tesis_posgrado/Pdf/Aaron_Clemente_Lacayo_A.pdf
- Laudon, K. & Laudon, J. (1995). *Administración de los Sistemas de Información*. México: Editorial Mc Graw – Hill Interamericana de México S.A.