UNIVERSIDAD DEL BIO BIO

Facultad de Ciencias Empresariales

Departamento de Administración y Finanzas

UNIVERSIDAD DEL BÍO-BÍO

MEMORIA PARA OPTAR AL TITULO DE CONTADOR PÚBLICO Y AUDITOR

"MANUAL DE IMPLEMENTACION DE SEGURIDAD DE INFORMACION TI PARA PYMES"

ALUMNA:

Karina Ramirez García

PROFESOR GUIA:

Juan Maldonado Riquelme

CONCEPCION, 2016

AGRADECIMIENTOS

En primer lugar quiero agradecer a mi familia por el apoyo incondicional en este proceso y sobre todo a lo largo de todos los años de estudio, los cuales han sido difíciles pero los he sabido sobrellevar.

A los distinguidos Docentes de la Universidad del Bío Bío por entregarme los conocimientos adquiridos durante toda la etapa de estudio, a mi Profesor Guía Señor Juan Maldonado por su orientación y apoya a la realización de mi Tesis.

A nuestros compañeros (as) por su buena interacción y solidaridad.

Sin duda dar gracias a dios por la orientación, por sentir su apoyo incondicional en todo momento de mi vida y en esta etapa tan importante de mi vida.

Karina Ramirez García

INDICE

Contenido

RESUMEN EJECUTIVO

La presente investigación es sobre un "manual de implementación de seguridad de información TI para pequeñas y medianas empresas" ya que la seguridad de información es un tema de gran importancia en todas las empresas en la actualidad, porque día a día la tecnología avanza para ayudar tanto a las personas como a las empresas a tener mejores resultados, pero esto también conlleva tener mayores cuidados e implementar seguridad de información para el uso de TI, puesto que existen vulneraciones que pueden dañar gravemente a las organizaciones.

En esta investigación se han definido como debe ser la seguridad de información con los puntos importantes tratados en este manual, se identifican las amenazas y vulnerabilidades que existen, posteriormente se entregan los controles para prevenir las amenazas presentadas, luego se evalúan los controles que se implementaron para saber si están funcionando de forma correcta y por último se entrega información que la gerencia puede optar a considerar o no.

Las tecnologías de información se han vuelto parte de la vida de todas las personas sin poder evitarlas porque están en todas partes y son una herramienta de suma importancia para realizar las funciones de cualquier organización por pequeña que sea, permitiendo generar, recopilar, intercambiar, procesar y ayudando a tomar decisiones que vayan en beneficios siendo analizadas dependiendo de las necesidades que presenta la empresa a través del tiempo, ya que la cantidad de información que se produce es inmensa sin importar el tamaño de la empresa o el rubro que tenga.

Para que se pueda implementar cualquier sistema de información y que se genere seguridad de información para PYMES debe existir voluntad por parte de la gerencia y todos quienes componen el negocio para aprender de que se trata, que involucra, quienes forma parte y que rol cumple para el apoyo de la empresa. Todo va en directo apoyo a cualquier medida de seguridad que se busque introducir la administración.

INTRODUCCION

La presente investigación trata sobre "Manual de implementación de seguridad de información TI para PYMES", generando una investigación al respecto en cuanto a la situación de las Pymes en chile frente a la seguridad de información, que tienen escasamente implementadas en su organización o en muchos casos no tienen conocimiento de esto, por lo que esta investigación busca entregar una herramienta clara y de forma resumida que ayude a generar una cultura de seguridad de información dentro del negocio para mejorar el cuidado que le deben dar a la información ya que es su activo más importante.

Se busca acercar el tema a las pymes y que mediante este documento puedan llevar a cabo una implementación con nociones básicas por la gerencia o dueños de la empresa sin tener que contratar a una persona especializada para la implementación e invertir recursos que son limitados o predeterminados para otras áreas. La presente investigación se encuentra dividida en 4 puntos para la mejor comprensión.

En el primer capítulo se entrega los conceptos básicos que tiene que saber el lector para entender la información que se entrega a continuación.

En el segundo capítulo se da a entender porque es importante la seguridad de información y sus aspectos claves dentro de este trabajo.

El tercer capítulo aborda de forma directa el "Manual de implementación de seguridad de información TI para Pymes" el cual es la base que tendrán para ayudar a su empresa a resguardar todo lo que usado de mala forma puede perjudicar enormemente a su negocio.

Ya llegando al cuarto y último capítulo se puede ver los resultados obtenidos de la encuesta, ayudando a generar los diferentes puntos de vistas que se expresan en las respuestas de las preguntas. Dando a entender la importancia de esta investigación y diseño del manual para toda empresa que tiene interés en cuidar cada una de las áreas de su organización.

PLANTEAMIENTO DEL PROBLEMA

Durante las dos últimas décadas el crecimiento de las tecnologías se ha disparados siendo cada vez más requerido su uso para el desarrollo de la vida tanto personal como laboral, debido a la explosión, del uso de aparatos tecnológicos que se encuentran en el mercado de buena calidad y bajos precios, ha provocado que las personas se sientan seducidas e impulsadas por el entorno a convertirse en usuarios de la tecnología pudiendo comunicarse, divertirse y una infinidad de opciones para acceder dentro de un mismo aparato como lo son los celulares inteligentes con sistema operativo androids, computadores portátiles (notebook) o Tablet pudiendo utilizarlos para cualquier fin que el usuario quiera darle sin limitaciones, con acceso a internet en conjunto con las diferentes aplicaciones disponibles que ayudan a muchas tareas cotidianas permitiendo generar y obtener la información.

Con este avance producido también ha dado origen a la creación del concepto de tecnologías de información dado el constante flujo de información que emerge de las herramientas tecnológicas, llegando a las personas de forma independiente o a través de organizaciones para facilitar tareas y procesos ayudando a la producción, pero también ha incitado que personas externas traten de vulnerar las barreras de acceso para obtener información altamente sensible de las organizaciones que pueden perjudicar gravemente la imagen y muchas cosas más. Esto ha hecho que sea imprescindible tomar decisiones al respecto para proteger su negocio.

JUSTIFICACION DEL PROYECTO

Dado el constante uso de las tecnologías de información ha provocado que todas las empresas quieran o no, hayan tenido que ir modificando como guardaban su información y también en que guardaban su información, si antes como muchos saben o recuerdan la información financiera o cualquier otra se registraba de forma manual y después se dejaba en bodegas o habitaciones donde solo la gerencia o encargados de finanzas tenían acceso a ella, ahora con toda la tecnología al alcance de cualquier persona ha hecho que las organizaciones también se vayan actualizando comparando computadoras y así a medida que va apareciendo nuevos aparatos se vaya traspasando la información dejándola en nubes virtuales para que se pueda descargar desde cualquier punto que necesiten las personas del negocio como lo es el gerente o los dueños, pero esto también ha provocado que hayan aparecido personas que buscan vulnerar sistemas de información por diversión o lo más peligrosos con fines maliciosos que pueden llegar a causar graves daños filtrando información importante.

Siendo un punto muy importante el resguardo de su información es que este proyecto busca acercar de una forma sutil para quien lea esto, entienda que la seguridad de información se puede implementar tomando medidas básicas pero muy eficaces y que pueden ser mantenidas en el tiempo, para esto se toma reconocidos libros que tratan muy bien el tema de seguridad, enfatizando en los puntos importantes porque una implementación de seguridad adecuada requiere mucho tiempo, personal especializado e inversión que muchas veces no tienen para dedicar a este tipo de áreas.

Considerando todo lo anterior se explican las amenazas, se entienden y se dan las herramientas para combatir las vulnerabilidades que se encuentren en los sistemas.

OBJETIVO GENERAL

Esta investigación tiene por objetivo entregar conocimientos de amenazas de seguridad de información que pueden afectar a las pequeñas y medianas empresas (Pymes) ya que cuentan con recursos más limitados y el personal contratado se limita hacer el trabajo para el cual fue reclutado por ende en muchas ocasiones no existe los profesionales idóneos para preocuparse de esta área, por eso el manual que se diseño puede ser leído por cualquier empleado, el gerente o algún inversionista y ser entendido porque se expresan las amenazas a las cuales más están expuestos y las soluciones para combatirlos teniendo en cuenta controles y evaluaciones a la seguridad de información de la empresa.

OBJETIVOS ESPECÍFICOS

Para lograr dicho objetivo general se deberán lograr los siguientes objetivos específicos:

- ✓ Base de conocimientos con las buenas prácticas de seguridad informática para Pymes.
- ✓ Descripción de la Pyme
- ✓ Matriz de riesgo de evaluación de madurez se seguridad TI basada en COBIT.
- ✓ Estudio de sensibilización de la alta gerencia a los riesgos expuestos.
- ✓ Diseño del manual de implementación de seguridad de información TI para Pymes.

METODOLOGIA

Para realizar esta investigación se analizó el capítulo 5 de CISA para entender cómo implementar una adecuada seguridad de información, entendiendo las amenazas, controles y posteriores evaluaciones para saber si se están llevando a cabo correctamente los controles. Posterior al análisis se hace una encuesta a un grupo de PYMES de la región que poseen sistemas de información automatizados, abarcando un grupo amplio de la industria, de los cuales se puede mencionar:

- Comercio de confección de ropa de hombre.
- Venta de repuestos de motocicletas y accesorios.
- Venta de lencería para hombre y mujer.
- Venta de comida rápida.

Diseño de estudio: tipo cuantitativo descriptivo-explicativo.

Objetivo de estudio: Creación de manual de implementación de seguridad de información TI para PYMES: se utilizó el capítulo 5 de manual de preparación para examen CISA (certified information systems auditor) es una certificación para auditores respaldada por la Asociación de Control y Auditoría de Sistemas de Información (ISACA) (Information Systems Audit and Control Association) en el cual se expresar todos los cuidados que se debe tener al evaluar una auditoria TI, por lo tanto se toma como una gran ayuda para tener una seguridad de información de los activos de información.

El proceso de estudio se lleva a cabo a través de las siguientes etapas:

- ✓ Primera etapa: se llevó a cabo una recopilación de información mediante la revisión bibliográfica.
- ✓ Segunda etapa: se desarrollaron los contenidos fundamentales sobre la seguridad información TI.

- ✓ Tercera etapa: se elaboró una encuesta, basada en los estándares y buenas prácticas de la seguridad de los sistemas de información y se aplica a las PYMES, seleccionando un grupo de la región, para saber situación actual y conocimientos que tiene en el tema.
- ✓ Cuarta etapa: se realiza la confección del "Manual de implementación de seguridad de información TI para PYMES".

Procesamiento de los datos:

Para el procesamiento y análisis de los datos se utilizan estadísticas descriptivas a través del software Microsoft Excel.

CAPITULO I: "CONCEPTOS GENERALES"

1. MARCO TEORICO

Para introducirnos al tema primero se debe entender lo que son las PYMES, se definen según la "Biblioteca del congreso nacional de chile" como "pequeña y mediana empresa". Adicionalmente la ley hace las siguientes definiciones:

Microempresa: Empresas cuyos ingresos anuales por ventas y servicios y otras actividades del giro, no hayan superado las 2.400 UF en el último año calendario.

Pequeña empresa: Empresas cuyos ingresos anuales por ventas y servicios y otras actividades del giro, sean superiores a 2.400 UF, pero inferiores a 25.000 UF en el último año calendario.

Mediana empresa: Empresas cuyos ingresos anuales por ventas y servicios y otras actividades del giro, sean superiores a 25.000 UF, pero inferiores a 100.000 UF en el último año calendario.

Adicionalmente, para efectos laborales, se hace la siguiente clasificación según números de trabajadores:

Microempresas: Empresas que cuentan con uno a nueve trabajadores.

Pequeñas empresas: Empresas que cuentan con 10 a 49 trabajadores.

Medianas empresas: Empresas que cuentan con 50 a 199 trabajadores.

Las PYMES, componen más del 63% del empleo a nivel nacional (http://www.mipymes.cl/2014/chile-es-el-sexto-pais-donde-mas-crecieron-los-prestamos-pyme) (fecha de estudio realizado por la OCDE en 2012).

Cada vez se ha vuelto más indispensable el uso de computadores y de las diferentes herramientas tecnológicas que diariamente están al alcance, lo cual ha tenido un incremento significativo en el transcurso de los últimos 20 años dando paso a lo que hoy en día se conoce como tecnologías de información (TI) siendo su uso e implementación indispensable en un mundo donde las tecnologías ya son parte significativa de muchas personas a través de todo el mundo, siendo parte de sus vidas debiendo convivir y recurrir a estas ya que cada vez encuentran nuevas formas de llegar a los usuarios generando una relación estrecha desde el primer momento siendo una gran herramienta de ayuda.

El crecimiento del uso de tecnologías no se ha debido solamente porque existan tecnologías pensadas de forma individual para las personas las cuales han sido muy exitosas hasta la actualidad, sino que también ha estado enfocada en las empresas para solventar necesidades presentes o que se van presentando conforme pasa el tiempo siendo indispensable evaluaciones de las herramientas ya existentes y de las personas que la manipulan para saber si las tecnologías están de acuerdo a los requerimientos de la empresa y se tiene el conocimiento adecuado para dicha labor porque todo el avance tecnológico ha provocado que personas internas como externas se aprovechen de sistemas vulnerables o se especialicen para introducir amenazas que puedan afectar la continuidad del negocio.

Al ser las tecnologías de la información un elemento tan importante es inevitable no contar con ellas, las PYMES debe protegerlas como principal prioridad, sin embargo al hablar de seguridad de información es necesario entender que muchas empresas no invierten porque tiene altos costos mantener un área que esté a cargo de la seguridad TI, sus recursos son limitados y usados en otras áreas que consideran de mayor importancia por eso este estudio busca contribuir dando una solución frente a los recursos limitados con que cuentan los empresarios, es fundamental que los estándares internacionales estén alineados con las metas del negocio, ya que han sido diseñados dado la necesidad de tener un adecuado control de seguridad TI que se pueda sostener e ir modificando en el tiempo dependiendo de las necesidades que vaya presentando la empresa, con directo beneficio tanto para mejorar toda

la eficiencia de los procesos que se desarrollan dentro del negocio y frente a posibles fiscalizaciones de entes fiscales o privados contratados por la gerencia para evaluar los recursos de TI.

2. CONCEPTOS GENERALES

Para entender el siguiente estudio se considera muy importante y necesario definir algunos conceptos básicos que serán usados en dicha investigación.

SISTEMAS DE INFORMACION

Existen diversos significados en la actualidad de lo que es un sistema de información pero he elegido el siguiente:

Un sistema de información se puede definir técnicamente como un conjunto de componentes relacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar a la toma de decisiones y el control en una organización.

Esto plantea el instituto tecnológico de sonora en la Introducción a los sistemas de información.

Todo sistema de información tiene cuatro funciones básicas:

Estrada de información: Es el proceso mediante el cual el Sistema de Información toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o automáticas. Las manuales son aquellas que se proporcionan en forma directa por el usuario, mientras que las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos. Esto último se denomina interfaces automáticas.

Las unidades típicas de entrada de datos a las computadoras son las terminales, las cintas magnéticas, las unidades de diskette, los códigos de barras, los escáner, la voz, los monitores sensibles al tacto, el teclado y el mouse, entre otras.

Almacenamiento de información: El almacenamiento es una de las actividades o capacidades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede

recordar la información guardada en la sección o proceso anterior. Esta información suele ser almacenada en estructuras de información denominadas archivos. La unidad típica de almacenamiento son los discos magnéticos o discos duros, los discos flexibles o diskettes y los discos compactos (CD-ROM).

Procesamiento de Información: Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida. Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados. Esta característica de los sistemas permite la transformación de datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general de un año base.

Salida de Información: La salida es la capacidad de un Sistema de Información para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, terminales, diskettes, cintas magnéticas, la voz, los graficadores y los plotters, entre otros. Es importante aclarar que la salida de un Sistema de Información puede constituir la entrada a otro Sistema de Información o módulo. En este caso, también existe una interface automática de salida. Por ejemplo, el Sistema de Control de Clientes tiene una interface automática de salida con el Sistema de Contabilidad, ya que genera las pólizas contables de los movimientos procesales de los clientes.

SEGURIDAD DE INFORMACION

Para llegar a comprender que es seguridad de información debemos entender primero que existe la **PROTECCION DE ACTIVOS DE LA INFORMACION**, la cual:

Se ocupa de los componentes claves que aseguran confidencialidad, integridad y disponibilidad (**CIA**) de los activos de información.

Dentro de COBIT también conocidas como las buenas prácticas, CIA es muy importante ya que ayuda a satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control:

La **Confidencialidad**: se refiere a la protección de información sensitiva contra revelación no autorizada.

La **Integridad**: está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

La **Disponibilidad**: se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

ESTANDARES Y BUENAS PRACTICAS DE SEGURIDAD DE INFORMACION

Estos conceptos conviven muy bien ya que aborda la seguridad de información desde un mismo punto, teniendo pequeñas diferencias.

Estándar: Es un conjunto de reglas estandarizadas que contienen un catálogo de requisitos. Estos requisitos se refieren tanto a productos como a procesos. La estandarización recoge los deseos, las propuestas de todas las instituciones relevantes como son los fabricantes, las asociaciones de consumidores, los juristas, los centros de investigación, las entidades de certificación e inspección.

Sin estas normas sería impensable la actual circulación de mercancías, ya que cada uno de los productos debería ser examinado de acuerdo a unos criterios específicos. Existen en diferentes niveles y con distinto alcance.

• Estándares a nivel nacional, como por ejemplo: – los estándares DIN en Alemania (Deutsches Institut für Normung)

• Estándares a nivel europeo (estándares EN en la UE)

• Estándares Internacionales como por ejemplo los estándares IEC y las normas ISO reconocidas por un gran número de naciones en el mundo.

Buenas practicas: los objetivos de control para la información y la tecnología relacionada (cobit®) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de cobit representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por ti, aseguran la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

ESTANDARES BASICOS QUE REPRESENTAN LAS BUENAS PRACTICAS

Para muchas organizaciones es importante cuidar la información y tecnologías que las soportan porque representan los activos más importantes que tienen, pero en muchas ocasiones no se comprende bien, por esto existen vulneraciones en la seguridad y controles que no abarcan una adecuada protección. Para esto se ha creado estándares y buenas prácticas que ayudan a tener un marco de referencia que sirve para que la calidad y resguardo de la información sea llevado a cabo de la mejor forma.

A continuación se presentara un pequeño resumen de los estándares y buenas prácticas que todas las organizaciones deben usar para mejorar la seguridad de su información.

Dentro de las buenas prácticas quien mejor la representa es COBIT (Los Objetivos de Control para la Información y la Tecnología relacionada) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Estas prácticas ayudarán a optimizar el gobierno TI, asegurar la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

Para COBIT la información debe basarse en requerimientos, los cuales se amplían a la calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

• La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

• La eficiencia consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.

• La confidencialidad se refiere a la protección de información sensitiva contra revelación no autorizada.

• La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

• La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

• El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

• La confiabilidad se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

En cuanto a la seguridad de información dentro de los más completos manuales se encuentra CISA.

La asociación de auditoría y control de sistemas de información (ISACA en inglés) ha sido la encargada de crear el Manual para el examen CISA (Certified Information Systems Auditor).Se utiliza este manual en esta investigación porque abarca todas las áreas en la cuales debemos poner atención para la protección de la información y la tecnología que respaldan los procesos del negocio, es un complemento muy importante que se enseña a los auditores a encontrar y prevenir posibles defectos en cuanto a controles no adecuados o que no han ido renovándose en el tiempo, ya que en la actualidad son muchos los puntos en los cuales debemos poner atención frente a posibles amenazas que pongan en riesgo el negocio.

A medida que ha pasado el tiempo los diferentes países y sus mercados han tenido que ir creando y seguir estándares que aseguren la calidad de productos y servicios que son tranzados diariamente en el comercio internacional, por esto debido a la evaluación de las tecnologías de la información (TI) se han creado las conocidas ISO.

Como los siguientes:

ISO 27001: Proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

ISO 17999: Proporciona una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

AUDITORIA TI

Existen 7 tipos de auditoria que se pueden realizar, sin embargo en esta investigación la auditoria que más nos importa es la auditoria SI, la cual está enfocada en evaluar los Sistemas de Información.

Auditoria SI: "Este proceso recolecta y evalúa la evidencia para determinar si los sistemas de información y los recursos relacionados protegen adecuadamente los activos, mantienen la integridad y la disponibilidad de los datos y de los sistemas, proveen información relevante y confiable, logran de forma efectiva las metas organizacionales, usan eficientemente los recursos y tienen en efecto controles internos que proveen una certeza razonable que los objetivos del negocio, operacionales y de control serán alcanzados y que los eventos no deseados serán prevenidos o detectados y corregidos de forma oportuna.

POLITICAS DE SEGURIDAD

Se encuentran muchas definiciones pero se enfocan en el área que se utilizaran las políticas de seguridad.

Elegí esta definición porque se acerca más al tema tratado en esta investigación," políticas de seguridad es el conjunto de normas y procedimientos establecidos por una organización para regular el uso de la información y de los sistemas que la tratan con el fin de mitigar el riesgo de pérdida, deterioro o acceso no autorizado a la misma".

CAPITULO II: "IMPORTANCIA DE LA SEGURIDAD EN LAS TECNOLOGIAS DE INFORMACION"

INTRODUCCION

Cada vez toma más relevancia el cuidado que se debe dar a la información que se maneja dentro de una empresa, entendiendo que la protección del que es considerado su activo más importante es necesaria para que el negocio siga adelante y no se vea obligado a dejar de entregar sus servicios o productos por un robo de información importante o un ataque a sus herramientas tecnológicas, pero para llevar a cabo esto se debe entender que no tan solo se debe cuidar mediante protocolos o medidas impuestas para proteger la información, sino que también se debe entender que para tener éxito uno de los principales pilares; es el personal, quien debe estar informado para tomar las medidas adecuadas que vayan en directo beneficio del negocio evitando que amenazas externas puedan dañar la información que almacenan los sistemas de información que se encuentran en computadores o en línea mediante plataformas virtuales.

Es de vital importancia que se invierta en seguridad tanto en capital como capacitando a los empleados, ya que ellos son los que están en contacto directo de forma habitual y pueden identificar cualquier anomalía actuando de forma inmediata y oportuna. Por esto una vez que la empresa decide tener un control adecuado con políticas de seguridad TI se debe tomar en cuenta todo lo que abarca este nuevo cambio el que traerá muchos beneficios pero también metas en cuanto a poder sostenerlo en el tiempo, estableciendo medidas que ayuden a ir actualizando y reforzar controles que puedan estar vulnerables.

Para llevar un control eficiente que ayude al negocio se debe empezar por entender que es la seguridad de información, que se está buscando con estos cambios y que todos los que componen el negocio sepan porque de estos cambios, capacitarlos frente a estos nuevos ajustes es la mejor manera para una comprensión rápida y oportuna.

Con el avance del tiempo y entendiendo que en un mundo en el cual mucha de la información es transmitida, guardada y sostenida vía internet es imprescindible estar en conocimiento de los avances que diariamente se están dando a conocer respecto a la seguridad de información para establecer planes de contingencia frente a posibles amenazas y medidas de mitigación que respalden a las medidas de control previamente establecidas para proteger la información y las

tecnologías de información que soportan el flujo constante de información proveniente del interior y exterior de la empresa.

1. LA INFORMACION TOMADA COMO UN RECURSO ACTIVO DENTRO DE LA EMPRESA.

Muchas empresas consideran la información y las tecnologías como su activo más importante, sin embargo esto también ha provocado que muchas veces sean poco entendidos, para lograr obtener los mayores beneficios se debe considerar que la información debe ser resguardada ante cualquier evento que pueda ocurrir siendo de vital importancia que se cree consciencia TI, por esto al pasar del tiempo y con el avance en los sistemas de información (SI) se han dado cuenta la gerencia y quien está a cargo de la toma de decisiones de lo importante que es la seguridad dentro de la empresa.

Los entes que componen la alta gerencia han comprendido que el impacto significativo de la información a influenciado directamente en el éxito del negocio ha entendido que se debe alinear las buenas practicas que ayudan a establecer la seguridad con las estrategias de la empresa, debiendo invertir más en el cuidado, prevención y mitigación de riesgos TI.

Tanta importancia a tomado la seguridad de información que se han creado requerimientos regulatorios de los controles de TI, son múltiples los beneficios de adoptar correctamente medidas de control como por ejemplo optimizar los costos cuando sea posible mediante enfoques estandarizados en vez de enfoques especiales.

Cada empresa es diferente en todo ámbito, pero los estándares han sido creados por un conjunto de expertos los cuales abarcan desde el sector público al privado y todo tipo de servicio entregado por el negocio, por lo tanto los controles deben ser siempre evaluados con el paso del tiempo, ya que los requerimientos pueden cambiar y las necesidades de la empresa pueden ser distintas o entes fiscalizadores pueden cambiar las regulaciones existentes en la actualidad.

2. IMPORTANCIA DE LOS SISTEMAS DE INFORMACION.

Los sistemas de información (SI) son imprescindibles para toda empresa privada o pública porque sostienen el recurso más importante el cual es la información. Este término siempre ha estado presente desde hace mucho tiempo, a pesar de esto muchas veces se utiliza erróneamente como sinónimo de "Sistema de información informático" si bien esto ha sido en parte porque en la mayoría de los casos los recursos materiales de un sistema de información están constituidos casi en su totalidad por sistemas informáticos, pero no siempre esto ocurre aunque casi en su totalidad es así, pero se debe entender que los sistemas informáticos son una subclase o enlace que ayuda a llevar a cabo un SI , por esto mucho de lo que nos rodea es un sistema de información con un flujo constante de información que hace que genere respuestas dependiendo de nuestras necesidades. Siendo más conocidos a través del siglo XX y teniendo un fugaz ascenso dentro de los últimos 20 años de la mano con la evolución de las herramientas tecnológicas, esto ha provocado que en los últimos años ha crecido la cantidad de SI conocidos.

Como fue presentado anteriormente en el capítulo I la definición que elegí es la siguiente: "Un sistema de información se puede definir técnicamente como un conjunto de componentes relacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización."

Otro concepto pero que se refiere a seguridad computacional en un sistema de información esta descrito por tres componentes:

- Interfaces: permiten el intercambio de información con el mundo no digital, tales como teclados, altavoces, monitores, escáneres, impresoras, etc.
- Repositorios: almacenan los datos permanente o temporalmente, tales como buffers, RAM (memoria de acceso aleatorio), discos duros, caché, etc.
- Canales, que conectan los repositorios entre sí, tales como "buses", cables, enlaces inalámbricos, etc. Una red de trabajo es un conjunto de canales físicos y lógicos.
- Comportamiento:

- ✓ Mensajes, que acarrean un contenido o significado hacia los usuarios internos o servicios.
- ✓ Servicios, los cuales proveen algún valor a los usuarios o a otros servicios mediante el intercambio de mensajes.

Anteriormente nombradas en el capítulo I las actividades de un sistema de información son 4 las cuales se definirán brevemente:

- **Entrada de Información**: Captura o recolecta datos en bruto tanto del interior de la organización como de su entorno externo.
- **Almacenamiento de Información**: Guardar de forma estructurada la información recopilada.
- **Procesamiento de Información**: Convierte esa entrada de datos en una forma más significativa
- **Salida de Información**: Transfiere la información procesada a las personas o roles que la usarán.

CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN

Para que una empresa un sistema de información es fundamental ya que nace, se desarrolla y muere junto a la organización, muchos SI no necesariamente se implementan en forma computacional pero es la mejor herramienta que está a nuestro alcance para guardar y obtener lo que necesitemos. Por esto al diseñar un nuevo SI se debe considerar muchas cosas que afectan a la empresa y que sea siempre un aporte que ayude a obtener beneficios sin transformarse en algo complicado que utilizar, comprender y modificar dependiendo la necesidad requerida.

Existen pautas básicas para el desarrollo de un SI para la organización:

- **Codificación:** Con el algoritmo ya diseñado, se procede a su reescritura en un lenguaje de programación establecido (programación) en la etapa anterior, es decir, en códigos que la máquina pueda interpretar y ejecutar.

- Conocimiento de la Organización. Analizar y conocer todos los sistemas que forman parte de la organización, así como los futuros usuarios del SI. En las empresas (fin de lucro presente), se analiza el proceso de negocio y los procesos transaccionales a los que dará soporte el SI.

- Determinar las necesidades. Este proceso también se denomina licitación de requerimientos. En el mismo, se procede identificar a través de algún método de recolección de información (el que más se ajuste a cada caso) la información relevante para el SI que se propondrá.

- Diagnóstico. En este paso se elabora un informe resaltando los aspectos positivos y negativos de la organización. Este informe formará parte de la propuesta del SI y, también, será tomado en cuenta a la hora del diseño.

- Diseño del sistema. Una vez aprobado el proyecto, se comienza con la elaboración del diseño lógico del SI; la misma incluye: el diseño del flujo de la información dentro del sistema, los procesos que se realizarán dentro del sistema, el diccionario de datos, los reportes de salida, etc. En este paso es importante seleccionar la plataforma donde se apoyará el SI y el lenguaje de programación a utilizar.

- Identificación de problemas y oportunidades. El segundo paso es relevar las situaciones que tiene la organización y de las cuales se puede sacar una ventaja competitiva (Por ejemplo: una empresa con un personal capacitado en manejo informático reduce el costo de capacitación de los usuarios), así como las situaciones

desventajosas o limitaciones que hay que sortear o que tomar en cuenta (Por ejemplo: el edificio de una empresa que cuenta con un espacio muy reducido y no permitirá instalar más de dos computadoras).

- Implementación. Este paso consta de todas las actividades requeridas para la instalación de los equipos informáticos, redes y la instalación de la aplicación (programa) generada en la etapa de Codificación.

- Mantenimiento. Proceso de retroalimentación, a través del cual se puede solicitar la corrección, el mejoramiento o la adaptación del SI ya creado a otro entorno de trabajo o plataforma. Este paso incluye el soporte técnico acordado anteriormente.

- Propuesta. Contando ya con toda la información necesaria acerca de la organización, es posible elaborar una propuesta formal dirigida hacia la organización donde se detalle: el presupuesto, la relación costo-beneficio y la presentación del proyecto de desarrollo del SI.

Como ya se dijo un sistema de información siempre debe ir en beneficio ayudando a facilitar tareas y pudiendo obtener información confiable que pueda ser utilizada por los usuarios que la requieren para ayudar a la toma de decisiones.

3. POLITICAS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACION.

Las políticas de seguridad son un elemento clave dentro de un sistema de información y como la presente investigación está enfocada en la seguridad que debemos tener en las tecnologías de información (TI).

Se puede definir como "el conjunto de normas y procedimientos establecidos por una organización para regular el uso de la información y de los sistemas que la tratan con el fin de mitigar el riesgo de pérdida, deterioro o acceso no autorizado a la misma."

Según el grado de madurez de la organización en la gestión de sus activos de información, esta Política de Seguridad puede ser más o menos sistemática y detallada.

De una política de mínimos, que regule exclusivamente algunos aspectos del tratamiento de la información, como el alta y baja de usuarios y el acceso de los mismos a los sistemas de la Organización, podemos encontrarnos con una política de detalle ligada a una definición clara de roles y responsabilidades que desarrolle todo un sistema de gestión de la seguridad.

Para las empresas es muy importante tener políticas de seguridad bien definidas ya que esto puede evitar errores futuros que perjudiquen directamente a la organización a través de sus empleados, se han visto muchos casos de robo de información la cual ha sido sustraída por el propio personal para venderla a la competencia, todo esto a echo que sea imprescindible establecer procedimientos que mitiguen estos posibles casos que intenten perjudicar el desarrollo de las labores de la empresa.

Pero a pesar de que se tomen medidas de seguridad para proteger la información ningún sistema es cien por ciento seguro, porque mantener la seguridad total es a base de un alto costo, lo cual son pocas más empresas que pueden hacer esto, siendo las PYMES las que cuentan con menores recursos para establecer políticas que puedan controlar todo para no ser víctimas de *hackers.* La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

4. POLITICAS INTERNACIONALES DE SEGURIDAD DE INFORMACION

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

La norma ISO/IEC 17799 es una guía de buenas prácticas que ofrece instrucciones y recomendaciones para la administración de la seguridad, ofreciendo una estructura para identificar e implementar soluciones para riesgos específicos.

ISO 27001: Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones.

5. CONOCIMIENTO ADECUADO DE LOS USUARIOS DE SISTEMAS DE INFORMACION.

Es muy importante que los usuarios ya sea quien opera los sistemas o quien consulta a ellos estén informados para utilizar el sistema de forma eficiente siendo una ayuda a sus labores,

facilitando datos que serán entregados en forma rápida y cuando sea solicitada por cualquier empleado o persona externa sin tener que retrasar las tareas de otro trabajador al consultar sobre dicha información que se desea obtener. Para ayudar a entender el SI es necesario capacitarlos cuando se desea establecer un nuevo método de apoyo y mejora constante, todo en directo beneficio del avance de la organización frente a un mercado que cada vez es más Competitivo utilizando todas las herramientas tecnológicas al alcance para mejorar la producción y el desempeño de sus empleados.

6. IMPORTANCIA DE INCULCAR UNA CULTURA DE SEGURIDAD DE INFORMACION DENTRO DE UNA ORGANIZACIÓN

Toda nueva idea o proyecto que busque implementar la gerencia dentro de cualquier empresa u organización debe ser discutida en conjunto con todos los trabajadores, planteando porque se busca introducir esta nueva idea, que beneficios traerá, tiempo de implementación, medidas a tomar antes de implementar como ordenar cierta información para transición de forma segura y sin generar un desequilibrio dentro de la empresa el cual pueda generar un retraso en la producción de productos o servicios que entrega.

La comprensión de todas las personas que constituyen la empresa será fundamental para introducir el concepto de seguridad de información TI dentro de las políticas de la organización, dando respuestas a las dudas que irán surgiendo en el momento o también a largo plazo, teniendo la gerencia, área TI o administración un plan de reacción que facilite el flujo de información, tiempos, todas las áreas y personal que abarca estas medidas a tomar.

Todo contribuirá al desarrollo e implementación de la seguridad de información TI en las políticas de la empresa, las cuales se tratan en el manual que se presenta a continuación.

CAPITULO 3: "MANUAL DE IMPLEMENTACION DE SEGURIDAD DE INFORMACION TI PARA PYMES"

MANUAL DE IMPLEMENTACION DE SEGURIDAD DE INFORMACION TI PARA PYMES

INTRODUCCION

En chile la protección de la información se ha vuelto cada vez más importante por que como se ve día a día la información se puede transformar en un arma que en muchos casos destruye la reputación y afecta de forma muy negativa a quien se ve involucrado, ya sea para una persona publica o alguien de más bajo perfil que represente a una empresa, en cualquier momento la información puede ser vulnerada, si bien en los tiempos actuales no hay una forma exacta de controlar la seguridad de información que sea 100% efectiva, hay medidas que se pueden tomar para minimizar el riesgo que representa la fuga de información relevante.

Por eso el siguiente manual busca tratar este tema desde el punto de vista de una Pymes que no cuenta con tantos recursos como lo es una gran empresa que tiene departamentos y personas especializadas a cargo de la seguridad TI, invirtiendo grandes sumas de dinero para mantener su información salvaguardada. En el siguiente manual se busca entregar herramientas básicas de fácil comprensión que vayan en directo beneficio del negocio contribuyendo al mejor funcionamiento interno y entregando una imagen del compromiso adquirido por la gerencia preocupándose de todas las áreas que componen su organización entregando seguridad frente a posibles auditorias futuras.

Dichas medidas pueden ser aplicadas no necesariamente por un experto en seguridad de información sino que este manual esta echo para que los dueños, los inversionistas o la gerencia pueda implementarlas entendiendo para que sirven y en que benéfica a la empresa poner en practica dichas medidas de control.

OBJETIVO DEL MANUAL

El siguiente documento busca ser un manual de procedimientos para evaluar y llevar a cabo prácticas que ayuden a tener un control efectivo sobre sus activos de información, poniendo gran énfasis en medidas básica que se pueden implementar de forma segura y sin grandes costos para la administración, exponiendo riesgos que muchas veces se pasan por alto hasta que ocurre algo que puede perjudicar al negocio. Por eso, lo explicado a continuación contribuirá al desarrollo de tomar precauciones frente a peligros constantes del ambiente que los rodea y será el primer paso para salvaguardar la información que se encuentra vulnerable con mejoras constantes a través del tiempo o con el crecimiento de la empresa.

USUARIOS DEL MANUAL

Toda persona interesada en aprender y proteger su empresa como lo es la gerencia, administración, dueños, inversionistas, empleado o también algún interesado en crear su propia empresa e implementar seguridad de información. Este manual está hecho para una fácil comprensión pudiendo cualquier persona leerlo y entender las medidas básicas para la implementación de seguridad de información y pudiendo evaluarla mediante un modelo de madurez proporcionado por COBIT conocido también, como las buenas practicas.

IMPORTANCIA DEL MANUAL DENTRO DE LA ORGANIZACIÓN

Cada organización funciona de forma distinta, sin embargo desde hace años muchas empresas se han dado cuenta de lo importante que es tener una seguridad de información TI que vaya acorde al mercado he ir actualizándose de forma periódica para minimizar riesgos que puedan ocasionar graves daños a la empresa, sin embargo esto no ha surgido de forma espontánea he individual sino que ha sido a través de políticas internacionales que se han creado con la participación de diferentes expertos para llegar al consensó de medidas de seguridad de información que protejan de intrusos y malas prácticas que se han llevado por años en todo el mundo.

Cada medida implementada nunca será suficiente ya que al mismo tiempo que surgen ideas para el resguardo de la información, también surgen ideas que buscan vulnerar y causar daño robando información valiosa, sin embargo en este manual se busca entregar medidas básicas para la protección de su información y que sea el primer pie para seguir he ir avanzando día a día en la búsqueda de protección he ir creando una consciencia de seguridad de información TI, ya que las tecnologías no se detendrán en su avance creando nuevas ventanas que permitan el acceso de personas maliciosas en contra de todo lo que se ha construido dentro de una organización.

Antes de comenzar a leer este manual se debe asegurar los siguientes puntos:

- Debe existir disposición de las personas que trabajar dentro del negocio para aprender y entender por qué se están implementando estas medidas ya que ellos serán los usuarios de las medidas implementadas.
- Se debe estructurar las relaciones dentro de la empresa de forma que ayude al manejo TI con diferentes medidas.
- Nunca olvidar que quien utiliza las herramientas tecnológicas tanto en el interior y exterior de la empresa son personas por lo tanto sus acciones en muchos casos no se pueden controlar, por lo tanto siempre la gerencia debe estar preparada frente a posibles vulneraciones voluntarias e involuntarias.
- Todo proceso que vaya en beneficio de la organización debe ser revisado de forma periódica para aplicar mejoras necesarias para resguardar la información más relevante.
- Se busca generar una consciencia de seguridad de información dentro de la organización.

SEGURIDAD DEL ENTORNO

PASO 1: CONOCIMIENTO DE PROCEDIMIENTO A RESGUARDAR

Es importante saber los accesos al sistema, a quien se les han otorgado y que grado de acceso tienen, controlar el personal que ha entrado y ha salido de la empresa para otorgar o terminar los accesos correspondientes, establecer y orientar a todo el personal la seguridad que se busca obtener.

Dentro del trabajo

La gerencia se debe encargar de que los usuarios nuevos y los ya existentes tengan claro las políticas de seguridad de la empresa para minimizar todos los riesgos, por esto se debe proveer a todos los empleados, contratistas y terceros usuarios un nivel adecuado de consciencia, educación y entrenamiento en los procesamientos de seguridad y el uso correcto de facilidades de procesamiento de información para minimizar posibles riesgos de seguridad.

Administración de seguridad de información

Para lograr una seguridad de información que se mantenga apoyando los procesos y actividades de la empresa se necesita un fuerte compromiso y soporte por parte de la alta gerencia para brindar entrenamiento de seguridad y para que la política de seguridad este por encima de la eficiencia. Este compromiso debe estar respaldado por un programa exhaustivo de entrenamiento formal en la consciencia de la seguridad. Esto puede requerir un entrenamiento especial a nivel de la gerencia, ya que la seguridad no es necesariamente parte de los conocimientos y experiencia de la gerencia. El entrenamiento en seguridad para diferentes funciones dentro de la organización necesita ser adaptado para resolver necesidades específicas de seguridad.

De los siguientes puntos se debe preocupar la gerencia o área de recursos humanos de la empresa porque a partir de ellos se crea la primera seguridad de información:

- *Privacidad*

La privacidad es el acatamiento de la confianza depositada y la obligación en relación con cualquier información relativa a una persona identificada o identificable.

Privacidad es un asunto de toda la organización que, por su naturaleza, requiere un enfoque consistente y homogéneo a través de toda la organización. Por lo tanto, debe ser introducida sistemáticamente en las políticas, estándares y procedimientos desde el comienzo mismo. Es importante que la gerencia evalué con recursos propios o contrate servicios externos para saber el nivel de privacidad que hay dentro de la organización.

- *Filtrado*

Se deberían efectuar verificaciones de los antecedentes de todos los candidatos a empleo, contratistas y terceros usuarios en conformidad con las leyes, regulaciones y ética relevantes, esto tomando en cuenta los requerimientos del negocio, la clasificación de la información a ser accedida y los riesgos percibidos. Se debería efectuar un proceso de filtrado para los contratistas y los terceros usuarios. Donde se proveen contratistas a través de agencia, el contrato con la agencia debería especificar claramente las responsabilidades de la agencia para filtrar y los procedimientos de notificación que ellos necesitan seguir si no se ha efectuado el filtrado o si los resultados dieran motivo para dudar o preocuparse. Del mismo modo, el contrato con el tercero debería especificar claramente todas las responsabilidades y los procedimientos de notificación para el filtrado.

- *Terminación de empleo*

Cada vez que un empleado sale de la empresa se debe asegurar protocolos y controles para que exista devolución de los equipos y todas las herramientas de trabajo que ayudaron en su labor, como también todos los accesos de sistema que se habían entregado. Es muy importante revisar y que haya información fluida para informar de cambios en el personal.

PASO 2: IDENTIFICACION DE VULNERABILIDADES Y AMENAZAS

Existen diversas vulnerabilidades asociadas al acceso físico que se tratan más adelante, por lo tanto no serán mencionadas ahora.

PASO 3: CONTROLES

Los nuevos usuarios de TI

Los nuevos usuarios de TI y, en general todos los nuevos empleados a los cuales se les asignan PCs u otros recursos deben ser informados de sus principales obligaciones de seguridad que los fuerza a cumplirlas. Estos son:

- ✓ Leer y acordar seguir las políticas de seguridad.
- ✓ Mantener en secreto los logon ID y las contraseñas.
- ✓ Bloquear sus pantallas de terminal cuando no estén en uso.
- ✓ Reportar las violaciones de seguridad que se sospechan.

Acceso de empleado terminado

La terminación de empleo puede ocurrir en las siguientes circunstancias:

- ✓ A solicitud del empleado (renuncia voluntaria del servicio).
- ✓ Programada (al retiro o terminación del contrato).
- ✓ Involuntaria - forzada por la gerencia en circunstancias especiales.

Cuando ocurre la renuncia involuntaria de empleo, los derechos de acceso lógico y físico de los empleados a la infraestructura de TI deben ser restringidos o retirados a la brevedad para que el empleado una vez terminado el contrato no tenga acceso a información de la empresa.

Recursos a utilizar para tener seguridad

A continuación se entregar diferentes controles para las amenazas presentadas anteriormente con el objetivo de prevenir o mitigar riesgos.

Bases de seguridad

Para tener un plan básico de seguridad pretende ser usado como un primer paso a la seguridad de TI. El plan básico debe ser seguido por una evaluación y en el futuro con un plan completo de seguridad sería lo ideal.

Recomendaciones para la seguridad básica de TI		
Tópicos	**Objetivos**	**Recomendaciones**
Inventario	Establecer y mantener un inventario.	Se espera que los usuarios sigan las normas para manejar las computadoras conectadas a la red, y que tengan direcciones de red registradas. El sistema operativo y el dueño deben estar incluidos junto con los datos suministrados.
Antivirus	Instalar software antivirus con actualización automática.	El software antivirus con archivo digital automático DAT debe ser actualizado de forma regular, siendo por lo menos una vez por semana.
Contraseñas	Reconocer la importancia de las contraseñas.	Los usuarios deben usar solamente contraseñas fuertes. El departamento de TI en el caso que corresponda debe suministrar orientación para las contraseñas, si no existe un departamento especializados TI entonces la gerencia debe ser la encargada de aconsejar y preocuparse de las contraseñas generadas por los empleados.

Patching	Hacerlo automático: menos trabajo para usted, menos probabilidades de falla.	Lo ideal en toda empresa es que exista en cada máquina una configuración de parcheo automático para el sistema operativo y para el parcheo básico del software. Se debe configurar un proceso que funcione para el departamento y que minimice las interrupciones en horas inconvenientes. Las estaciones de trabajo deben estar más automatizadas para permitir a los administradores de sistemas el tiempo para dar a los servidores la atención requerida para minimizar el impacto sobre los servicios ofrecidos.
Minimizar los servicios ofrecidos por los sistemas	Eliminar los servicios innecesarios reduciendo el riesgo se seguridad y ahorrando tiempo en el largo plazo.	Para mejorar la seguridad básica y minimizar el esfuerzo para mantener los sistemas, las estaciones de trabajo deben ofrecer solamente los servicios que se necesiten. Muchos sistemas operativos están instalados con los servicios activos.
Resolviendo vulnerabilidades	Permitir una fácil recuperación de los errores del usuario y de las fallas de hardware con copias de respaldo.	Los compromisos del sistema pueden consumir mucho tiempo y dañar la credibilidad y la integridad. La información del escaneo de toda la empresa ayuda a identificar las vulnerabilidades en cada sistema y a proveer una línea base para

		comparación cuando la integridad del sistema está en juego.
Copias de respaldo	Permitir una fácil recuperación de los errores del usuario y de las fallas de hardware con copias de respaldo	Las copias de respaldo deben hacerse en el sitio alterno para mayor seguridad.

ACCESOS AL SISTEMA

PASO 1: CONOCIMIENTO DE PROCEDIMIENTO A RESGUARDAR

Dentro de toda empresa es de suma importancia tener control de quien tiene acceso y a que información está teniendo acceso para tener una adecuada seguridad de información.

El permiso de acceso al sistema es la prerrogativa para hacer algo con un recurso computarizado o informático. Esto, por lo general, se refiere a un privilegio técnico, por ejemplo, la capacidad de leer, crear, modificar o eliminar un archivo o dato, ejecutar un programa, o abrir o usar una conexión externa.

El acceso a los recursos de sistemas de información, se establece, gestiona y controla a nivel físico y/o lógico.

Controles de acceso físico al sistema restringen la entrada y la salida del personal a un área como por ejemplo un edificio de oficinas, una sala, un centro de proceso de datos o una habitación que contenga equipo de procesamiento de información. Existen un sin fin de tipos de controles de acceso físico, que incluyen tarjetas de identificación, tarjetas inteligentes, llaves de custodia, barreras construidas de piso a techo, cerraduras y biométrica.

Controles de acceso lógico se encargan de restringir los recursos lógicos del sistema (transacciones, datos, programas, aplicaciones) y se aplican cuando se necesita el recurso

objeto. En base a la identificación y a la autenticación del usuario que requiere un recurso dado y analizando los perfiles de seguridad del usuario y del recurso, es posible determinar si se debe permitir el acceso solicitado, es decir, que información puede ser utilizada por los usuarios, los programas o transacciones que ellos pueden ejecutar, y las modificaciones que pueden hacer. Dichos controles pueden estar integrados en el sistema operativo, invocados a través de un software independiente de control de accesos e incorporados en programas de aplicación, sistemas de base de datos, dispositivos de control de la red y utilitarios / utilidades del sistema.

El acceso físico o lógico a la información del negocio debe ser establecida con el máximo de criterio y enfocándose en lo que necesita la empresa resguardar, que medidas establecerá ya que existe un sin número, como también se debe tomar en cuenta los recursos con que cuenta la gerencia para implementar los diferentes controles de acceso.

Para un mayor entendimiento los activos de TI bajo la seguridad lógica pueden agruparse en cuatro capas, las redes, las plataformas (sistemas operativos), las bases de datos y las aplicaciones. Esto permite el concepto de seguridad en capas para acceso al sistema que proporciona un mayor alcance y granularidad de control de los recursos de información.

Todo este planteamiento debe existir desde un principio para trazar los puntos a seguir en la implementación de seguridad de información.

Identificadores de inicio de sesión (Login ID) y contraseña

Los login IDs y las contraseñas son los componentes del proceso de identificación y autenticación de un usuario, donde la autenticación se basa en algo que uno sabe. Cada login debe registrarse para acceder de forma individual, no en grupo.

Principales características de las contraseñas

Una contraseña debe ser fácil de recordar para el usuario que la creo pero debe tener un grado de dificultad para que sea difícil de adivinar para el intruso que quiere acceder a información.

Las contraseñas pueden ser entregadas por los encargados de seguridad TI, por la administración o la gerencia. Por lo general al acceder la primera vez al sistema pide automáticamente el cambio de clave para asegurar la confidencialidad.

Si se entra/teclea una contraseña equivocada un numero predefinido de veces, por lo general tres, Logon-ID debe ser desactivado automáticamente y de manera permanente (solo el administrador puede desbloquear el ID) o temporalmente (el sistema desbloquea el ID después de un periodo de tiempo previamente especificado).

Principales puntos para estar atento:

- ✓ Las contraseñas deben ser cambiadas periódicamente.
- ✓ La contraseña deber ser cambiada en su lugar de trabajo en ningún otro sitio donde se pueda ver su contraseña.
- ✓ Las contraseñas son únicas por persona.

La seguridad de los recursos humanos y terceros

Deben estar implementadas practicas adecuadas de seguridad de información para asegurar que los empleados, contratistas y terceros usuarios entienden sus responsabilidades, y son aptos para los roles para los que son considerados, y para reducir el riesgo de robo, fraude o abuso de puntos vulnerables.

PASO 2: IDENTIFICACION DE VULNERABILIDADES Y AMENAZAS

Exposiciones y controles de acceso físico

Cualquier problema de acceso físico es una preocupación importante para el negocio por que puede tener perdida financiera, repercusiones legales, la pérdida de credibilidad o la perdida de ventaja competitiva. A continuación se describen algunas exposiciones y sus posibles perpetradores.

Exposiciones de acceso físico

Las exposiciones que se exponen son a causa de violación accidental o intencional de las vías de acceso incluye las siguientes:

- ✓ Entrada no autorizada

- ✓ Daño, vandalismo o robo de los equipos o documentos
- ✓ Copia o visualización de información sensitiva o patentada
- ✓ Alteración de equipos e información sensitivos
- ✓ Revelación al público de información sensitiva
- ✓ Abuso de los recursos de procesamientos de datos
- ✓ Chantaje
- ✓ Fraude

Posibles perpetradores

Los posibles perpetradores incluyen a los empleados que tienen acceso autorizado o no autorizado que están:

- ✓ Descontentos (irritados o preocupados por alguna acción emprendida por la organización o por la gerencia de esta).
- ✓ En huelga
- ✓ Amenazados con una acción disciplinaria o con despido.
- ✓ Son adictos a una sustancia o al juego.
- ✓ Están experimentando problemas financieros o emocionales.
- ✓ Se les haya notificado su despido.

Otros posibles perpetradores podrían incluir:

- ✓ Ex – empleados
- ✓ Personas ajenas interesadas o informadas, como por ejemplo los competidores, ladrones, el crimen organizado y los hackers.

- ✓ El ignorante accidental – una persona que sin saberlo, comete una violación (podría ser un empleado o una persona ajena).

La fuente más probable de exposición es de persona no informada, ya sea de forma accidental o porque no sabe pero el impacto mayor puede venir de las personas que tiene intenciones maliciosas y buscan perjudicar a la organización.

PASO 3: CONTROLES

Controles de acceso físico

Los controles de acceso físico están hechos para proteger a la empresa de accesos no autorizados, siendo muy importante que estos controles estén limitados a los accesos autorizados por la gerencia. Esta autorización puede ser explicita, como en una cerradura de puerta para la cual la gerencia le haya autorizado a usted para tener una llave; o implícita, como en la descripción de un puesto de trabajo que implica una necesidad de tener acceso a reportes y a documentos sensitivos.

Ejemplos más comunes de los controles de acceso:

- ✓ Bitácora o registro manual – se debe exigir que todos los visitantes firmar en un libro de vistas indicando su nombre, de que compañía vienen, motivo de su visita y a quien van a ver. Este registro se hace generalmente en la recepción y a la entrada de las computadoras si la situación de la empresa lo permite.
- ✓ Cámaras de video – las cámaras deben estar ubicadas en puntos estratégicos y ser monitoreadas por algún guardia o la propia gerencia según sea la situación de la empresa.
- ✓ Guardias de seguridad – son muy útiles si prestan atención a las cámaras, personas ajenas que entran a salen del edificio o personas con actitudes sospechosas que anden merodeando por el lugar.

- ✓ Acceso controlado de visitantes – Todo visitante debe estar escoltado por algún empleado responsable de la empresa. Los visitantes incluyen amigos, vendedores de cualquier índole, consultores y auditores externos.

INTERNET

PASO 1: CONOCIMIENTO DE PROCEDIMIENTO A RESGUARDAR

Internet es un neologismo del inglés que significa **red informática descentralizada de alcance global**. Se trata de un sistema de redes informáticas interconectadas mediante distintos medios de conexión, que ofrece una gran diversidad de servicios y recursos, como, por ejemplo, el acceso a plataformas digitales.

Como tal, es un anglicismo que se forma por la abreviación del término *International Network of Computers*, que en español se podría traducir como **'Red Internacional de Computadoras'**, o también como 'Red de redes'.

Su origen data del año 1969, cuando se estableció la primera conexión entre computadoras de varias universidades de Estados Unidos.

En español, la palabra internet está considerada como un nombre propio. La Real Academia Española (RAE), en su diccionario, admite que se escriba con o sin mayúscula inicial. De allí que, preferentemente, se utilice sin artículo, aunque en caso de usarlo, se recomienda el uso femenino (la), ya que el nombre equivalente en español vendría a ser 'red', que es femenino.

Internet y World Wide Web (WWW o web)

En ocasiones, ambos términos se utilizan de forma indistinta, aunque técnicamente no tienen el mismo significado. Internet es el medio de transmisión que utiliza la *World Wide Web* o WWW (en español se suele utilizar el término web). De esta forma, uno de los servicios que Internet permite utilizar es la web, entendida como un conjunto de protocolos que permite el acceso a distancia de archivos de hipertexto.

Conexiones de internet

Las **conexiones de internet** son los **medios disponibles para que un usuario pueda utilizar los servicios que ofrece internet** a través de dispositivos que utilizan tecnología informática, como computadoras, *tablets* y teléfonos móviles.

Existen distintas maneras de acceder a internet. Algunas de ellas son la utilización de una línea telefónica (convencional o digital, por ejemplo, ADSL), la conexión por cable (a través de fibra óptica), la conexión vía satélite o la conexión a redes inalámbricas, también llamadas *wireless*.

PASO 2: IDENTIFICACION DE VULNERABILIDADES Y AMANEZAS

VULNERABILIDADES DE INTERNET

Factores que pueden favorecer un ataque en internet

Para que ocurran ataques tanto pasivos como activos tienen un lugar un número de razones, incluyendo:

- ✓ Disponibilidad de herramientas y de técnicas en internet o de software disponibles comercialmente que un intruso pueda descargar con facilidad.
- ✓ Falta de consciencia y entrenamiento sobre seguridad entre los empleados de una organización.
- ✓ Seguridad inadecuada sobre firewalls y sobre sistemas operativos que permite a los intrusos visualizar las direcciones internas y usar indiscriminadamente los servicios de red.

Para poder contrarrestar o impedir que se produzcan ataques que buscan hacer daño de cualquier forma que afectan el trabajo y un sin fin de actividades que se desarrollan dentro de una empresa se han creado apoyos para fortalecer las medidas de seguridad.

Crimen informático

Es muy importante que el área encargada de TI este en conocimiento de lo que es el crimen informático y que alcance puede tener, o de qué forma puede afectar a la organización. Los sistemas informáticos pueden ser usados para robar dinero, mercancías, software o información corporativa. También pueden cometerse crímenes cuando los datos o sistemas de aplicación son manipulados para que acepten transacciones falsas o no autorizados. Pero también existe otro modo más sencillo como lo es robo de equipos: robo físico…

Cometer crímenes que se aprovechan de la informática y la información que esta contiene puede ser perjudicial para la reputación, la moral y la existencia misma de una organización. Lo que puede provocar la pérdida de clientes, la vergüenza para la gerencia y las acciones legales contra la organización puede ser una consecuencia.

Entre las consecuencias se encuentras las siguientes:

- ✓ Pérdidas financieras
- ✓ Repercusiones legales
- ✓ Pérdida de credibilidad o ventaja competitiva
- ✓ Chantaje/ espionaje industrial
- ✓ Revelación de información confidencial, sensitiva o embarazosa
- ✓ Sabotaje

Es muy importante que la gerencia como cumplirá el rol de fiscalizar de forma interna sepa y entienda las diferencia entre crimen y abuso cibernético para sustentar las metodologías de análisis de riesgo y las prácticas de control relacionadas.

Las personas que pueden perpetrar estos crímenes son las siguientes:

- ✓ Hackers – Personas que tienen la habilidad de explorar en detalle para descubre las debilidades de un computador o de una red informática, siendo diferentes sus motivaciones para vulnerar dicha red.

- ✓ Script kiddies – son personas inexpertas que interfieren en los sistemas mediante el uso de herramientas automatizadas.
- ✓ Crackers – Personas que tratan de violar la seguridad del sistema, y ganan acceso al sistema de otra persona sin haber sido invitados.
- ✓ Empleados – (autorizados y no autorizados) – Miembros de la organización y a los que se da acceso al sistema basándose en las responsabilidades del puesto de trabajo, estas personas pueden causar daño considerable a una organización.
- ✓ Personal de SI – son las personas que están a cargo de custodiar la información por lo tanto tienen más acceso.
- ✓ Usuarios finales – usan el sistema con frecuencia por lo que tienen un buen conocimiento de la información de la organización y tiene fácil acceso a los recursos internos.
- ✓ Ex empleados – ya conocen la organización y pueden usar la información que conocen o utilizar accesos a los sistemas que no se hayan dado de baja por descuido de la gerencia o encargados de TI pudiendo provocar graves daños a la empresa.

En los tiempos actuales el cruce de información para resolver crímenes cibernéticos que se producen entre países ha crecido y ha mejorado potencialmente a resolver estos crímenes pero cuando son personas expertas utilizan barreras y diferentes tipos de métodos para protegerse cuidando de no ser encontrados.

Virus

Un virus es un término genérico que se emplea para referirse a muchos programas hechos para atacar un sistema operativo con el principal objetivo de hacer daño. Para que un virus pueda entrar en el sistema operativo de una computadora se auto programan a otros programas que pueden ser relativamente benignos, como por ejemplo desfase de aplicación de la web, o maliciosos, como borrar archivos, corrompiendo programas o causando negación de servicio.

Generalmente los virus atacan cuatro partes de la computadora:

- ✓ Archivos de programas ejecutables.
- ✓ El sistema archivo-directorio que rastreo la ubicación de todos los archivos de la computadora.
- ✓ Las áreas de autoarranque y del sistema que se necesitan para iniciar la computadora.
- ✓ Archivos de datos.

Otra forma muy parecida a un virus encontrado con frecuencia es un gusano, pero este a diferencia de un virus no se acopla a otro programa de forma física, sino que se encarga de explotar las debilidades de seguridad en las configuraciones de los sistemas operativos.

La transmisión de un virus o gusano puede ocurrir fácilmente por que ocupa internet, siendo el momento de bajar archivos a los buscadores web de las computadoras los momentos críticos y de riesgo frente a estos programas maliciosos. También los virus son fácilmente transmitidos adjuntos a un correo electrónico de modo que cuando el software de procesamiento de palabras abre el adjunto, el sistema se infecta, si no está usando software de escaneo para revisar los adjuntos sin abrirlos.

Amenazas y seguridad de internet

La naturaleza misma de internet la hace muy vulnerable ataques. Es un sistema global conectado entre redes públicas y privadas que permite comunicarse entre sí. En la actualidad las computadoras existentes y que están conectadas son muchas permitiendo intercambiar información, archivos, transacciones de forma rápida y lo más libre posible, ya no solamente se utiliza para fines comerciales y afines a un trabajo sino que también se utiliza como una red social para crear lasos de amistad o encontrarse con viejos amigos.

Impacto de las amenazas

Existen diversas amenazas como las mencionadas anteriormente siendo difícil determinar el impacto que podrían producir, pero dado la experiencia en seguridad de información a través del tiempo, podrían ocurrir los siguientes tipos de impactos que pueden perjudicar significativamente a la empresa:

- ✓ Pérdida de ingresos.
- ✓ Mayor costo de recuperación (corrigiendo la información y reestableciendo los servicios).
- ✓ Perdida de información (datos críticos, información propietaria, contratos).
- ✓ Perdida de secretos comerciales.
- ✓ Daño a la reputación.
- ✓ Incumplimiento de compromisos contractuales.
- ✓ Acción legal por parte de los clientes por pérdida de datos confidenciales.

Amenazas de seguridad inalámbrica y mitigación de riesgos

La clasificación de las amenazas de seguridad puede ser segmentada en nueve categorías:

- Errores y omisiones
- Fraude y robo cometido por usuarios automatizados y no autorizados del sistema
- Sabotaje por empleados
- Perdida de soporte físico y de infraestructura.
- Hackers maliciosos
- Espionaje industrial
- Código malicioso
- Espionaje de gobierno extranjero
- Amenazas a la privacidad personal

Los dispositivos inalámbricos son los que más riesgo tienen dado su portabilidad. Los usuarios autorizados y los no autorizados pueden cometer fraudes y robo; sin embargo es mucho más probable que los autorizados cometan estos actos puesto que cuentan con más accesos al sistema.

Los hackers maliciosos pueden causar mucho daño introduciéndose a un sistema para bombardearlo con virus, gusanos, caballos de Troya, bombas lógicas y algún software no deseado que está destinado a dañar archivos o a destruir un sistema.

PASO 3: CONTROLES

Son diversos los controles que se pueden implementar pero los más conocidos y fácil de entender son los siguientes:

Sistemas de seguridad Firewall (cortafuegos)

Al momento de conectar una computadora a internet se enfrenta a un alto peligro. Debido a que internet por su carácter de abierto hace que cualquiera que esté conectado pueda estar propenso a ser víctima de un ataque. Muchos hackers están atentos a cualquier descuido que pueda ocurrir dentro de una organización para vulnerar barreras establecidas para la protección de extraños que presentan puntos de falla o simplemente no existen barreras implementadas, ingresando de forma cautelosa y sin dar señales de su presencia pudiendo utilizar datos e información para diferentes fines.

Por esto motivos las empresas deben establecer firewall que le permitan generar un medio de seguridad perimetral para sus redes. De igual forma este principio aplica para los sistemas muy sensitivos o críticos que necesitan ser protegidos de usuarios internos dentro de la red corporativa en quienes no se confía (intrusos internos).

Los firewall son un dispositivo instalado en el punto de acceso donde las conexiones de la red entran a un lugar que aplica reglas para controlar el tipo de tráfico de red que fluye hacia dentro y hacia fuera.

Características generales de los firewalls

Los firewalls son una excelente herramienta de ayuda para la empresa que quiere controlar los accesos a internet, así también el acceso de las personas y de lo que pueden ver. Son combinaciones de hardware y software que se articulan usando enrutadores, servidores y una variedad de software. Para que tenga el resultado esperado se debe ubicar en el punto más

vulnerable entre una red corporativa e internet, pudiendo ser tan sencillo o tan complejo como lo exija la política corporativa de seguridad.

Algunas características de los firewalls:

- ✓ Bloquear el acceso a sitios particulares en internet.
- ✓ Impedir que determinados usuarios tengan acceso a ciertos servidores o servicios.
- ✓ Monitorear las comunicaciones entre una red interna y una externa.

Se pueden ampliar las funcionalidades de algunos firewalls de tal forma que puedan también proporcionar protección contra los virus y ataques dirigidos a explotar las vulnerabilidades conocidas del sistema operativo.

Tipos firewall

Generalmente los tipos de firewalls disponibles en la actualidad se pueden clasificar en tres categorías que incluyen.

- ✓ Filtrados de paquetes por medio de router.
- ✓ Sistemas de firewalls de aplicación.
- ✓ Inspección a nivel del estado.

Estos tipos de firewalls son discutidos en las siguientes secciones:

Firewalls de filtrado de paquete por medio de router

Uno de los tipos más sencillos y de los primeros tipos de firewall consistía en el filtrado de paquetes desplegados entre la red privado e internet.

Sistemas de firewall de aplicación

Los firewall de aplicación permiten que la información fluya entre los sistemas pero no permiten el intercambio directo de paquetes y permiten el flujo directo de paquetes entre los sistemas interno y externo.

Firewall de inspección de estado

Este sistema de inspección de estado mantiene la pista o la traza sobre la dirección de destino de IP de cada paquete que sale de la red interna de la organización. Con esto cada vez que se recibe la respuesta a dichos paquetes, se toma este registro como referencia para asegurarse que la respuesta a dicha solicitud sea correcta.

COMPUTACIÓN MÓVIL

PASO 1: IDENTIFICACION DE PROCEDIMIENTO A RESGUARDAR

En la actualidad en el ambiente de computación móvil es muy difícil implementar controles de acceso físico y lógico, existiendo diversos aparatos como lo son los laptop, Tablet, discos duros externos, pendrive y también los celulares inteligentes por lo cual no es extraño que en muchas ocasiones se guarde datos sensitivos. Para proteger la confidencialidad de los datos de la laptop requiere un método de seguridad en capas tanto a los niveles de acceso físico como lógico, así como también una política de seguridad y directrices de prácticas seguras para laptop.

PASO 2: IDENTIFICACION DE VULNERABILIDADES Y AMENAZAS

Como los laptops (computadoras portátiles) a menudo se usan para conectarse a distancia a los sistemas de computadoras de la organización, se debe tener cuidado especial para defenderse contra código malicioso.

PASO 3: CONTROLES

Controles para computación móvil

Los siguientes controles reducirán el riesgo de revelación de datos sensitivos almacenados en una laptop:

- ✓ Grabar o marcar un número de serie y nombre y logo de compañía en una laptop usando un grabador eléctrico o pegando coletillas resistentes.
- ✓ Encriptar datos usando software conocido de encripcion, que este basado en algoritmos de dominio público y que no sea patentado. La decisión de que encriptar se puede dejar

al usuario, creando volúmenes designados en los que se almacenan y procesan los archivos encriptados. Un método alternativo encripta todo el disco duro, no dejando nada a la discreción del usuario.

- ✓ Asignar contraseñas a archivos individuales para prevenir que sean abiertos por una persona no autorizada, una que no esté en posesión de la contraseña. Esta facilidad debe ser usada con gran precaución ya que si se olvidara la contraseña, o si la persona que lo creo se fuera de la organización, los datos no estarían disponibles porque la contraseña no puede ser evadida.
- ✓ Establecer un equipo de respuesta a robo y desarrollar procedimientos para continuar cuando una laptop fuera robada.

SEGURIDAD DE INFRAESTRUCTURA

PASO 1: IDENTIFICACION DE PROCEDIMIENTO A RESGUARDAR

Infraestructura

Para poder implementar seguridad de información TI acorde a su empresa es de suma importancia que la infraestructura sea adecuada para el control que se busca establecer.

Teniendo en la actualidad diversas herramientas tecnológicas que son muy conocidas de diferentes marcas, modelos, programas integrados, sistemas operativos en teléfonos celulares todo esto con una amplia calidad y precio para quien desea obtenerlos.

- Computador

Dicho lo anterior cada usuario debe tener un ordenador acorde a las necesidades que establece su trabajo, entregando como herramienta principal un computador en buen estado con mantenciones regulares y al momento recibirlo estar listo para comenzar a trabajar con las funciones básicas.

- Instalaciones

Las instalaciones donde se desarrollara el trabajo y donde se ubicara el ordenador debe estar acondicionado para dar comodidad y seguridad al personal que utiliza herramientas tecnológicas.

- Desarrollo y autorización de cambios de red

Cualquier cambio de configuración de la red para actualizar líneas de telecomunicación, terminales, módems y otros dispositivos de red deben ser autorizados por escrito por la gerencia e implementados a su debido tiempo, siempre debiendo ser supervisados.

Deben existir procedimientos específicos de desarrollo y control de cambios para el hardware y el software de los componentes de red.

Los procedimientos deben abarcar:

- Firewalls
- Routers
- Switches
- Topología de red/ DNS
- Software de cliente
- Software de administración de red
- Hardware y configuración de servidor web
- Software de aplicación
- Páginas web

PASO 2: IDENTIFICACION DE VULNERABILIDADES Y AMENAZAS

Las vulnerabilidades han sido nombradas anteriormente en el acceso lógico y el acceso físico.

PASO 3: CONTROLES

Seguridad de la infraestructura de la red

Las redes de comunicación incluyen generalmente dispositivos conectados a la red y programas y archivos que soportan las operaciones de la red.

Para un mejorar control y mantenimiento de la infraestructura y su uso, siendo la administración muy importante pero también se debe tomar en cuenta los registros que implican estos dispositivos con los de firewall.

Se puede llegar a mejorar la seguridad cuando se logra un inventario dinámico de los dispositivos, para saber cuándo ocurra un incidente saber que computadora fue y quien la uso.

Herramientas de ayuda para proteger información

Encriptado/ cifrado

La encripcion trata como el proceso de convertir un texto normal a una forma de texto codificado el cual no se puede leer a menos que el proceso se invierta se llama desencripcion. Para efectuar la desencripcion se hace por medio de una función matemática y de una contraseña especial de encripcion/desencripcion llamada clave.

La encripcion tiene limitaciones porque no puede impedir que se pierdan datos pero se debe considerar como una forma esencial pero incompleta de control de acceso que puede ser incorporado al plan de seguridad existente en la organización.

Firmas digitales

Una forma digital es una identificación electrónica de una persona o entidad creada usando un algoritmo de clave pública y que está destinada a verificar a un destinatario, la integridad de los datos y la identidad del remitente.

Sobre digital

Es utilizado para enviar información encriptada y la clave relevante junto con este. Es un método altamente seguro para enviar documentos electrónicos.

Riesgo de la encripcion y la protección de contraseñas

La seguridad de los métodos de encripcion se basa enteramente en el secreto de las claves, mientras más se uses una clave, más vulnerable se vuelve, ya que muchos hackers se han vuelto cada vez mejores para romper las contraseñas encriptadas.

El carácter aleatorio de la generación de claves es también un factor significativo en la capacidad para comprometer una clave. Cuando las contraseñas están ligadas a una generación de claves, utilizando palabras comunes es cuando más vulnerables se vuelven.

Computo forense

Por definición, el computo forense es "el proceso de identificar, preservar, analizar y presentar evidencia digital en una forma que sea aceptable en cualquier proceso legal (es decir, un tribunal).

Incluye actividades que involucran la exploración y aplicación de métodos para recolectar, procesar, interpretar y usar evidencia digital que ayuda a sustanciar si ha ocurrido un incidente, como por ejemplo:

- Proveer validación de que un ataque en efecto ocurrió.
- Recolectar evidencia digital que pueda ser usada posteriormente en procesos judiciales.

Cualquier documento electrónico o dato puede ser usado como evidencia digital siendo muy importante que la evidencia sea original y no este alterada.

Muchas organizaciones no están acostumbradas a tratar con intrusos y crímenes electrónicos, respondiendo a estos eventos solo cuando se presentan no teniendo procedimientos idóneos para enfrentar estas situaciones.

Protección de datos

Para prevenir que la información buscada sea altera, deben existir todas las medidas posibles. Es muy importante que se informe a todas las partes que se busca información y no deben borrar correos electrónicos ni nada que pueda servir como evidencia y contribuya a la investigación.

Controles técnicos

Se pueden implementar métodos técnicos de prevención de virus a través de medios de hardware y software. Las siguientes son tácticos de hardware que pueden reducir el riesgo de infección:

- ✓ Usar protección de virus de reinicio (Boot).
- ✓ Usar reinicio (Booting) remoto.
- ✓ Usar una contraseña basada hardware.
- ✓ Usar los disquetes con la protección contra escritura.
- ✓ Asegurar que los protocolos inseguros sean bloqueados por el firewall contra segmentos externos e internet.

PROBLEMAS Y EXPOSICIONES AMBIENTALES

PASO 1: IDENFICACION DE PROCEDIMIENTO A RESGUARDAR

Las exposiciones ambientales se deben principalmente a acontecimientos que ocurren naturalmente, como por ejemplo, tormentas eléctricas, terremotos, erupciones volcánicas, huracanes, tornados y otros tipos de condiciones climatológicas extremas. Muchas fallas de energía pueden agruparse cuatro formas, basadas en la duración y relativa severidad de la falla:

- ✓ Falla total (apagón) – una pérdida total de energía, pudiendo abarcar un solo edificio o un área geográfica extensa, y con frecuencia es causada por condiciones climáticas o la incapacidad de una compañía eléctrica de responder a las demandas de sus clientes.
- ✓ Voltaje severamente reducido (caída de voltaje) – esto ocurre cuando una compañía de electricidad no suministra los voltajes adecuados, limitando la vida útil de los aparatos computacionales pudiendo causar un daño permanente.

- ✓ Depresiones, picos y voltajes – disminuciones (depresiones) o aumentos (picos y sobre voltajes) siendo temporales y presentando de forma súbita en los niveles de voltaje. Causando estas anomalías perdidas de datos, corrupción de datos o daño físico a dispositivos de hardware, como por ejemplo discos duros o chips de memoria.
- ✓ Interferencia electromagnética – causada por interferencia eléctricas o equipo eléctrico ruidoso (ejemplo, motores, iluminación fluorescente, transmisores de radio). Esta interferencia puede ocasionar que los sistemas de computadora se cuelguen o caigan, así como también daños similares a los ocasionados por las depresiones, picos y sobre voltajes.

Las interrupciones por periodos breves que abarcan un par de segundos pueden ser prevenidas usando protectores de voltaje debidamente colocados. Las interrupciones intermedias que duran desde algunos segundos hasta 30 minutos, se pueden controlar por medio de dispositivos de suministro ininterrumpido de energía (UPS). Finalmente, las interrupciones de larga duración, que duran de algunas horas hasta varios días, requieren el uso de generadores alternos de energía. Estos generadores pueden ser dispositivos portátiles o parte de la infraestructura del edificio según corresponda al tamaño y las necesidades del negocio, usan fuentes alternas de energía, como por ejemplo diésel, gasolina o propano.

Otra área importante trata del daño provocado por agua/ inundación siendo provocado por un fenómeno de la naturaleza o alguna cañería rota dentro del edificio de la empresa.

Otras preocupaciones fuera de todo lo dicho anteriormente trata del daño provocado por el hombre. Ellas incluyen amenazas/ataques terroristas, vandalismo, choque eléctrico y falla del equipo por acción de terceros.

PASO 2: IDENTIFICACION DE VULNERABILIDADES Y AMENAZAS

Se debe entender muy bien que amenazas representa un apagón o un sobre voltaje para las computadoras de la organización teniendo perdidas parciales o completas, que pueden

perjudicar el funcionamiento normal de la empresa, ya sea por unas horas o en casos más graves pudiendo llegar a ser días.

PASO 3: CONTROLES

Controles para las exposiciones ambientales
Las exposiciones ambientales deben asignarse el mismo nivel de protección que las exposiciones físicas y lógicas.

Extintores manuales de incendios
Los extintores manuales de incendios deben estar ubicados en lugares estratégicos de fácil acceso en todo el sitio. Deben cumplir con las normas de calidad y ser revisados una vez al año para ver su funcionamiento, y que no se encuentren vencidos.

Alarmas manuales de incendios
Para el buen funcionamiento de las alarmas deben estar ubicadas estratégicamente en todo el sitio. La alarma idealmente debiera estar conectada a una estación monitoreada por el guardia que cuida las instalaciones de la organización.

Detectores de humo
Los detectores humo para un funcionamiento óptimo es necesario que se sitúen por encima y por debajo del cielorraso en todo el sitio donde se encuentran los computadores pero esta medida debe ser aplicada a toda la infraestructura que compete al negocio para la protección de todo.

Protectores de voltaje
Estos dispositivos eléctricos reducen el riesgo de daño a los equipos debidos a variaciones de voltaje. Los estabilizadores de voltaje miden la corriente eléctrica que entra y aumenta o disminuye la carga de la misma para asegurar una corriente constante.

Planes documentados y probados de evacuación de emergencia.
Los planes de evacuación siempre deben poner énfasis en la seguridad humana, pero deben existir procedimientos para un cierre controlado de las computadoras en una situación de emergencia, si el tiempo lo permite.

POLITICAS DE PROCEDIMIENTOS

Para saber si los controles están funcionando deben existir políticas que cuide el buen funcionamiento de cada procedimiento implementado.

PASO 4:

Auditoria de la estructura de administración de seguridad de información

Frente a una auditoria es importante que la organización esté preparada porque se puede producir al momento en que un inversionista quiera invertir en la empresa y necesita saber el estado real de la seguridad de información que soporta los servicios y programas dentro de la empresa, también un proceso de auditoria se puede entender como un medio por el cual se sabe el estado en que se encuentra la organización para la toma de decisiones de la alta gerencia o el directorio, a medida que va creciendo la institución se hace cada vez más necesario las auditorias.

Revisar las políticas, procedimientos y estándares escritos

Dentro de toda asociación las políticas y procedimientos son la base que provee la estructura en conjunto con directrices a seguir para mantener las operaciones y la vigilancia de lo que ocurre. Por esto el auditor encargado de TI revisara las políticas y procedimientos examinando que se cumplan como están estipuladas por la gerencia.

Políticas de seguridad de acceso lógico

Como ya se había mencionado en un principio de este manual, el acceso lógico es muy importante porque es la primera barrera para acceder al sistema que resguarda la información, teniendo cuidado y prestando atención a quien se da determinados permisos, que acceso deber ser eliminado, ya sea porque no pertenece a la organización o por otra decisión tomada por quien esté a cargo de la protección TI.

Consciencia y entrenamiento formal de seguridad

La seguridad efectiva dependerá siempre de las personas que formas la organizacion. Como resultado, la seguridad solo puede ser efectiva si los empleados están en conocimiento de lo

que se espera de ellos y cuáles son sus responsabilidades. Deben saber porque existen las medidas de seguridad en la empresa y que pasaría si estas medidas de seguridad fueran violadas.

Propiedad de los datos

La propiedad de los datos se refiere a la clasificación de elementos de datos y asignar las responsabilidades para mantener la confidencialidad, siendo de importancia quien está a cargos del cuidado íntegro y exacto de dicha información.

Los propietarios de los datos

Estas personas son las encargadas de tener en su poder los datos resguardados siendo generalmente gerentes y directores responsables de usar información para ejecutar y para controlar el negocio.

Estándares de acceso

Al momento de una auditoria el auditor debe asegurarse que se estén cumpliendo las normas establecidas ayudando a cumplir los objetivos de la organización para la separación de funciones prevenir fraudes o errores y que cumplan con las políticas para minimizar riesgos de acceso no autorizado.

Los estándares de seguridad pueden definirse:

- ✓ A un nivel genérico (por ejemplo, todas las contraseñas debe tener por lo menos cinco caracteres de longitud).
- ✓ Para los sistemas específicos de aplicación (por ejemplo, los empleados del área de ventas pueden entrar a los menús para el ingreso de facturas de ventas pero no pueden entrar a los menús que permitan autorización de cheques).

Auditoria de acceso lógico

Cuando un auditor evalúa los controles de acceso lógico considera lo siguiente:

- ✓ Busca obtener un entendimiento general de los riesgos de seguridad que enfrenta el procesamiento de la información a través de una revisión de la documentación relevante.

- ✓ Documentar y evaluar los controles sobre las vías potenciales de acceso al sistema, examinando si son eficientes y efectivos poniendo énfasis en el software y hardware e identificando cualquier deficiencia.
- ✓ Probar los controles para comprobar que los accesos estén funcionando y se estén aplicando de una forma efectiva.
- ✓ Evaluar el ambiente de control de acceso para determinar que se están logrando los objetivos de control revisando las políticas escritas, observando las prácticas y los procedimientos.

Entrevistar al personal de sistemas

Para un mayor control y mantener los diversos componentes de las vías de acceso así como también el sistema operativo, a veces se debe recurrir al a expertos técnicos. Muchas veces estas personas pueden ser de gran ayuda porque pueden manejar valiosa información para que el auditor Ti pueda llegar a entender la seguridad. El auditor también se reúne con la gerencia para entender los organigramas y las descripciones de los puestos de trabajo.

Controles sobre los recursos de producción

Todos los controles de acceso a las computadoras deben extenderse más allá de los datos de aplicación y de las transacciones. Hay muchas utilidades de alto nivel, bibliotecas de macros o de control de trabajos, bibliotecas de control y parámetros de software del sistema para los que el control de acceso debe ser particularmente fuerte. El tener acceso a toda esta información puede dar la posibilidad de evadir muchos otros controles de acceso.

Revisar los controles de acceso y la administración de las contraseñas

Se revisan los controles de acceso y la administración de las contraseñas para determinar:

- ✓ Si existen algún procedimiento para agregar usuarios a la lista de acceso autorizado para utilizar los recursos de la computadora.
- ✓ Existen procedimientos que ayuden a que las contraseñas de las personas no sean vulneradas tan fácilmente.

- ✓ Si las contraseñas que se emiten tienen una longitud adecuada, si no son adivinadas con facilidad y no se repiten caracteres.
- ✓ Si las contraseñas se cambian periódicamente.
- ✓ Si los procedimientos proveen la suspensión de los códigos de identificación o la inhabilitación de la terminal, después de un número determinado de violaciones de los procedimientos de seguridad.

Auditoria al acceso físico

Para lograr un entendimiento general y una percepción de la instalación que se está inspeccionando es importante recorrer todo el lugar. Este recorrido puede ayudar mucho a saber cómo funcionan las restricciones de acceso físico (por ejemplo, control sobre los empleados, los visitantes, los intrusos y los proveedores).

Las siguientes vías de entrada física deben ser evaluadas para una seguridad apropiada:

- ✓ Todas las puertas de entrada
- ✓ Ventanas y paredes de vidrio
- ✓ Paredes movibles y cubículos modulares
- ✓ Por encima de los cielorrasos suspendidos y por debajo de los pisos falsos
- ✓ Sistemas de ventilación
- ✓ Por encima de una cortina, pared falsa.

TÉCNICAS DE INVESTIGACIÓN

Las técnicas de investigación incluyen los crímenes informáticos y la protección de evidencia.

Investigación de crimen de computadora

Muchas veces los crímenes de computadora no son reportados porque simplemente no son detectados. Cuando son detectados los crímenes muchas veces las compañías dudan en reportarlo porque genera mucha publicidad negativa para la imagen del negocio. Por esto la empresa busca arreglar lo que se encuentra vulnerable y no reportarlo para no perjudicar, siguiendo adelante.

Es difícil determinar un crimen de computadora por la poca evidencia física que queda, ya que en muchos países las leyes están hechas para perseguir un crimen físico. Para encontrar al responsable se debe llamar a expertos sin intervenir en nada la evidencia par que puedan trabajar y encontrar las fallas.

EVALUACION GERENCIA FRENTE A CONTROLES MEDIANTE RIESGO E IMPACTO

Matriz de riesgo e impacto

Esta matriz es creada con la finalidad de facilitar la tarea de la gerencia al momento de identificar que controles pueden afectar más a la empresa, dando asignaciones que representan el impacto que la gerencia dará a cada riesgo.

Determinación de impacto expresada a continuación:

BAJO	El daño que puede producir a la organización no será tan fuerte, ya que no pondrá en un riesgo latente la información relacionada con la empresa.
MEDIO	El daño que se puede producir amenaza con filtrar información que puede perjudicar a la empresa, pero mediante una revisión rutinaria puede ser solucionada rápidamente sin generar daños que no se pueden reparar.
ALTO	Riesgo inminente que perjudica gravemente a la organización y que puede generar daños difíciles de reparar.

PLANEAR Y ORGANIZAR

	IMPACTO	**BAJO**	**MEDIO**	**ALTO**
IMPACTO	Definir un plan estratégico de TI			
	Definir la arquitectura de la información			
	Determinar la dirección tecnológica			
	Definir los procesos, organización y relaciones de TI			
	Administrar la inversión en TI			
	Comunicar las aspiraciones y la dirección de la gerencia			
	Administrar recursos humanos de TI			
	Administrar la calidad			
	Evaluar y administrar los riesgos de TI			
	Administrar proyectos			

ADQUIRIR E IMPLEMENTAR

	IMPACTO	BAJO	MEDIO	ALTO
IMPACTO	Identificar soluciones automatizadas			
	Adquirir y mantener software aplicativo			
	Adquirir y mantener infraestructura tecnológica			
	Facilitar la operación y el uso			
	Adquirir recursos de TI			
	Administrar cambios			
	Instalar y acreditar soluciones y cambios			

ENTREGAR Y DAR SOPORTE

	IMPACTO	BAJO	MEDIO	ALTO
IMPACTO	Definir y administrar los niveles de servicio			
	Administrar los servicios de terceros			
	Administrar el desempeño y la capacidad			
	Garantizar la continuidad del servicio			
	Garantizar la seguridad de los sistemas			
	Identificar y asignar costos			
	Educar y entrenar a los usuarios			
	Administrar la mesa de servicio y los incidentes			
	Administrar la configuración			
	Administrar los problemas			
	Administrar los datos			
	Administrar el ambiente físico			
	Administrar las operaciones			

MONITOREAR Y EVALUAR

	IMPACTO	BAJO	MEDIO	ALTO
IMPACTO	Monitorear y Evaluar el Desempeño de TI			
	Monitorear y Evaluar el Control Interno			
	Garantizar el Cumplimiento Regulatorio			
	Proporcionar Gobierno de TI			

PLAN DE CONTINUIDAD Y CONTINGENCIA

PASO 5:
TENER CONOCIMIENTO DE QUE ES Y COMO LLEVAR A CABO UN PLAN DE CONTINUIDAD DEL NEGOCIO (solo si la gerencia está dispuesta)

Es importante que exista un conocimiento de cómo continuar la organización frente a hechos fuera del control de la gerencia y empleados, siendo muchas veces pasadas por alto, para esto se entregan puntos básicos a los cuales prestar atención para pensar y poner en práctica un plan de continuidad del negocio en caso de algún desastre o eventualidad que se pueda presentar y tengan nociones básicas entregando información de utilidad, y esperando que el negocio ponga énfasis en lo necesario para llevar a cabo un plan de continuidad con todo lo que esto puede implicar.

Plan de continuidad

La planeación de continuidad del negocio y la planeación de contingencia de los sistemas de información es un proceso que va en directo beneficio del negocio dirigiendo la respuesta desde simple emergencias hasta desastres totales.

Siendo la última del proceso poder responder mejor a incidentes que puedan impactar en la gente, las operaciones y la capacidad de entregar bienes y servicios al mercado.

Esta área presenta una visión general de los principios de BCP (por Business Continuity Planning) y DRP (por Disaster Recovery Planning) y específicamente las siguientes áreas:

- Los procesos de BCP y DRP
- Análisis de impacto al negocio
- Estrategias y alternativas de recuperación
- Pruebas de plan

- Respaldo y restauración
- Consideraciones de auditoria

Se busca enfocarse en los elementos clave que se requieren para que una organización se desempeñe para planear proactivamente, y administre, las consecuencias de un desastre.

En una empresa en la actualidad no puede evitar todas las formas de riesgo corporativo o de daño potencial. Una buena forma para establecer la supervivencia de una organización es establecer una cultura que identificara y administrara estos riesgos que podrían causarle que sufra.

Algunos ejemplos de estos riesgos corporativos incluyen:

- Incapacidad de mantener los servicios críticos al cliente.
- Daño en la participación de mercado, la imagen, reputación o marca.
- No poder proteger los activos de la compañía, incluyendo propiedad intelectual y personal.
- Falla de control del negocio.
- No poder cumplir los requisitos legales o regulatorios.

El objetivo principal de la continuidad del negocio / recuperación de desastres es permitir que un negocio continúe brindando sus servicios críticos en caso de una interrupción y que pueda sobrevivir a una interrupción desastrosa de sus sistemas de información.

El plana de continuidades principalmente una responsabilidad de la alta gerencia, ya que ella es la encargada de salvaguardar tanto los activos como la viabilidad de la organización, es ejecutado por las unidades del negocio y de soporte igual, para proveer un nivel mínimo de funcionalidad de las operaciones del negocio, inmediatamente después de que se produzca una interrupción, mientras se está llevando a cabo la recuperación. Este plan debe abarcar todas las funciones y los activos que se requieren para continuar como una organización viable.

La planificación de la continuidad del negocio toma en consideración:

- Las operaciones críticas que son más necesarias para la supervivencia de la organización.
- Los recursos humanos/materiales que las soportan.

Desastres y otras interrupciones

Los desastres son interrupciones que ocasionan que los recursos que los recursos críticos de información queden inoperantes por un periodo de tiempo, impactando adversamente las operaciones organizacionales. La interrupción podría durar desde carias horas hasta varios días, dependiendo de la extensión del daño a los recursos de información.

Un desastre puede ser por calamidades naturales, como por ejemplo terremotos, inundaciones, tornados, tormentas eléctricas severas, incendios, etc. Los cuales causas daños importantes a las instalaciones de procesamientos y a la localidad en general. Otros eventos desastrosos que causan interrupciones pueden ocurrir cuando los servicios esperados ya no son proporcionados a la compañía, como por ejemplo, el suministro de energía eléctrica, las telecomunicaciones, el suministro de gas natural u otros servicios provistos por externos. Un desastre podría también ser causado por eventos precipitados por seres humanos tales como ataques terroristas, ataques de hackers, virus o error humano.

Tratando con daños a la imagen, reputación o la marca

Los rumores pueden surgir de muchas fuentes incluso de forma interna. Pudiendo o no estar relacionadas con un incidente serio o con una crisis. Ya sean "espontaneo" o un efecto colateral de un problema de continuidad del negocio o recuperación de desastre, sus consecuencias pueden ser devastadoras. Una de las peores consecuencias de la crisis es la perdida de la confianza y de la buena voluntad.

Toda organización que experimenta un incidente mayor deberá considera y aplicar algunas mejores prácticas básicas. Independientemente de las consecuencias de un incidente (demora o interrupción del servicio, pérdidas económicas, etc.), de darse alguno; cualquier opinión pública o rumores negativos pueden ser muy costosos. Reaccionar de manera apropiada en público (o

para con los medio) durante una crisis no es sencillo. Se debe nombrar y preparar de antemano un vocero debidamente entrenado. Normalmente, el asesor legal o un funcionario de relaciones públicas es la mejor elección. Nadie, independientemente de su rango en la jerarquía de la organización, con experiencia del vocero, debe hacer declaraciones públicas.

Política de continuidad del negocio y recuperación de desastres

Una política de continuidad del negocio debe ser proactiva y abarcar controles preventivos, de detección y correctivos. El plan de continuidad del negocio (BCP) es el control correctivo más crítico. Depende de que otros controles sean efectivos, en particular la administración de incidentes, y respaldo de medios.

Los incidentes y sus impactos pueden, hasta un cierto punto, ser mitigados a través de monitoreo preventivo.

Esto requiere que el grupo de administración de incidentes tenga el personal adecuado, este debidamente respaldado y entrenado en administración de crisis y que el plan de continuidad del negocio este bien diseñado, documentado, probado en ejercicio, financiado y auditado.

Análisis del impacto al negocio

El análisis del impacto al negocio es un paso fundamental y crítico para desarrollas el plan de continuidad del negocio. Esta etapa implica identificar los diversos eventos que podrían tener un impacto sobre la continuidad de las operaciones y su impacto financiero, humano, legal y de reputación sobre la organización.

Para ejecutar esta etapa con éxito, se debe lograr un entendimiento de la organización, de los procesos claves del negocio y de los recursos de SI utilizados para soportarlos. Esta etapa requiere un elevado nivel de soporte por parte de la alta gerencia y la total participación del personal tanto de tecnología de información (TI) como de los usuarios finales.

Hay diferentes métodos para efectuar un análisis sobre el impacto del negocio. Unos de los más populares es el método de cuestionario, el cual implica desarrollar un cuestionario detallado y circulado a los usuarios claves tanto en las áreas de TI como de los usuarios finales. La información recopilada es tabulada y analizada.

Estrategias de recuperación

Una estrategia de recuperación es una combinación de medidas preventivas, de detección y correctivas.

La acción más efectiva seria:

- Donde sea posible, eliminar la amenaza completamente
- Minimizar la probabilidad de que ocurra
- Minimizar el efecto de una ocurrencia

Eliminar la amenaza y minimizar el riesgo de que ocurra pueden resolverse a través de la implementación de seguridad física y ambiental. Minimizar el efecto puede lograrse implementando una resiliencia (capacidad de volver al estado normal de operación luego de ocurrir un evento adverso) integrada a través de direccionamiento alternativo y redundancia.

Desarrollo de planes de continuidad del negocio y recuperación de desastres

Basado en la información recibida del BIA, el análisis de criticidad y estrategia de recuperación seleccionada por la gerencia, se debe desarrollar un plan detallado de continuidad del negocio y recuperación de desastre. Los diversos factores que se deben considerar mientras se desarrolla el plan son:

- Está preparado antes de un desastre cubriendo el manejo de respuestas a incidentes para resolver todos los incidentes que afecten los procesos y análisis del negocio.
- Procedimientos de evacuación
- Procedimientos para declarar un desastre
- Las circunstancias bajo las cuales se debe declarar un desastre. Todas las interrupciones no son desastres, pero un pequeño incidente, si no es resuelto a su debido tiempo o de manera apropiada puede conducir a un desastre.
- La clara identificación de las responsabilidades en el plan
- La clara identificación de las personas responsables de cada función en el plan.

- La clara identificación de información de los contratos
- La explicación paso por paso de la opción de recuperación
- La clara identificación de los diversos recursos requeridos para la recuperación y operación continúa de la organización.
- La aplicación paso por paso de la etapa de recuperación.

El plan deber ser documentado y escrito en un lenguaje sencillo comprensible para todos. Es común identificar los equipos de personal que son responsables de tareas específicas en caso de desastre.

Otros aspectos a tener en cuenta en el desarrollo del plan

El personal que debe reaccionar a los escenarios de desastres / interrupción es el responsable de los recursos más críticos. Por lo tanto, la participación de la gerencia y de los usuarios es vital para el éxito del de continuidad del negocio. Las tres divisiones principales que requieren participación en la formulación del plan de continuidad del negocio son los servicios de soporte, las operaciones del negocio y el soporte del procesamiento de la información.

Cuando se formule el plan, se deben incluir los puntos siguientes:

- Una lista del personal, con información de contacto, requerido para mantener las funciones criticas del negocio en el corto, mediano y largo plazo.

La configuración de las instalaciones físicas, escritorios, sillas, teléfonos, etc. que requieren para mantener las funciones criticas del negocio en el corto, mediano y largo plazo.

Respaldos de los suministros requeridos

El plan debe considera todos los suministros necesarios para la continuidad de las actividades normales del negocio durante el proceso de recuperación. Esto incluye procedimientos escritos detallados y actualizados que pueden ser fácilmente seguidos por el personal permanente y el contrato que no esté familiarizado con las operaciones estándar de recuperación.

Pruebas del plan

Las mayorías de las pruebas de la continuidad del negocio no llegan a una prueba a escala de las porciones operativas de la corporación.

La prueba debe ser programada durante un tiempo que minimice las interrupciones a las operaciones normales. Los fines de semana son generalmente un buen momento para llevar a cabo las pruebas. Es importante que los miembros clave del equipo de recuperación participen en el proceso de prueba y se les dé el tiempo necesario para poner todo su esfuerzo en ello. La prueba debe ocuparse de todos los componentes críticos y simular las condiciones reales de procesamiento en el periodo de tiempo más activo, aun si se lleva a cabo fuera de horas laborales.

Especificaciones

La prueba debe tratar de cumplir las siguientes tareas:

- Verificar si el plan de continuidad del negocio es completo y preciso
- Evaluar el desempeño del personal involucrado en el ejercicio
- Evaluar el entrenamiento y el conocimiento de los miembros del equipo de continuidad que no pertenece al negocio
- Evaluar la coordinación entre el equipo de continuidad del negocio y los vendedores externos y los proveedores
- Medir la habilidad y capacidad del lugar de respaldo para llevar a cabo el procesamiento prescrito.
- Evaluar la capacidad de recuperación de los registros vitales
- Evaluar el estado y la cantidad de equipo y de suministros que han sido reubicados en el lugar de recuperación.
- Medir el desempeño general de actividades operativas y de procesamientos de los sistemas de información relacionadas con el mantenimiento de la entidad de negocio.

Análisis de resultados

Es importante tener formas de medir el éxito del plan y de la prueba comparando con los objetivos planteados. Por lo tanto, los resultados deben ser calibrados en forma cuantitativa en oposición a una evaluación basada únicamente en la observación.

Las medias específicas varían dependiendo de la prueba y de la organización. Sin embargo, estas medidas generales usualmente aplican:

- Tiempo – el tiempo transcurrido para realizar las tareas prescritas, la entrega de equipo, la reunión de personal y la llegada a un lugar predeterminado.
- Cantidad – la cantidad de trabajo realizado en el lugar de respaldo por el personal de oficina y las operaciones de procesamientos de los sistemas de información.
- Conteo – el número de registros vitales llevados exitosamente al lugar de respaldo frente al número requerido, y el número de suministros y de equipo solicitado frente al efectivamente con el número de transacciones procesadas.
- Exactitud – la exactitud de la entrada de datos en el lugar de recuperación frente a la exactitud normal (como un porcentaje). También se puede determinarla exactitud de los ciclos reales de procesamientos mediante la comparación de los resultados salientes con los resultados para el mismo periodo procesado bajo condiciones normales.

CONCLUSION

Al finalizar este manual se busca haber generado un entendimiento de la implementación de seguridad de información TI con medidas básicas para que se pueda llevar a cabo una seguridad de información que vaya en directo beneficio de la protección de información valiosa que puede ser usada de mala forma, afectando gravemente a cualquier empresa.

Tomando en cuenta todos quienes intervienen para llevar a cabo dicho proceso se dan instrucciones de cómo implementar seguridad de información y que se debe considerar para llevarlas a cabo, con el adecuado conocimientos en las amenazas, controles y posterior evaluación, todo con directo beneficio en la protección de una área muy importante dentro de toda empresa que muchas veces no se considera pero que debe ser tan básica como cualquier otra existente.

CAPITULO 4: RESULTADOS OBTENIDOS

INTRODUCCION

En este capítulo se exponen los resultados obtenidos gracias a la cooperación de un grupo de empresas PYMES que accedió a colaborar en dicha investigación con el objetivo saber cómo se encuentran de informadas estas empresas.

Los resultados obtenidos se describen a continuación de acuerdo a los 4 dominios del instrumento:

1.- Planear y organizar.

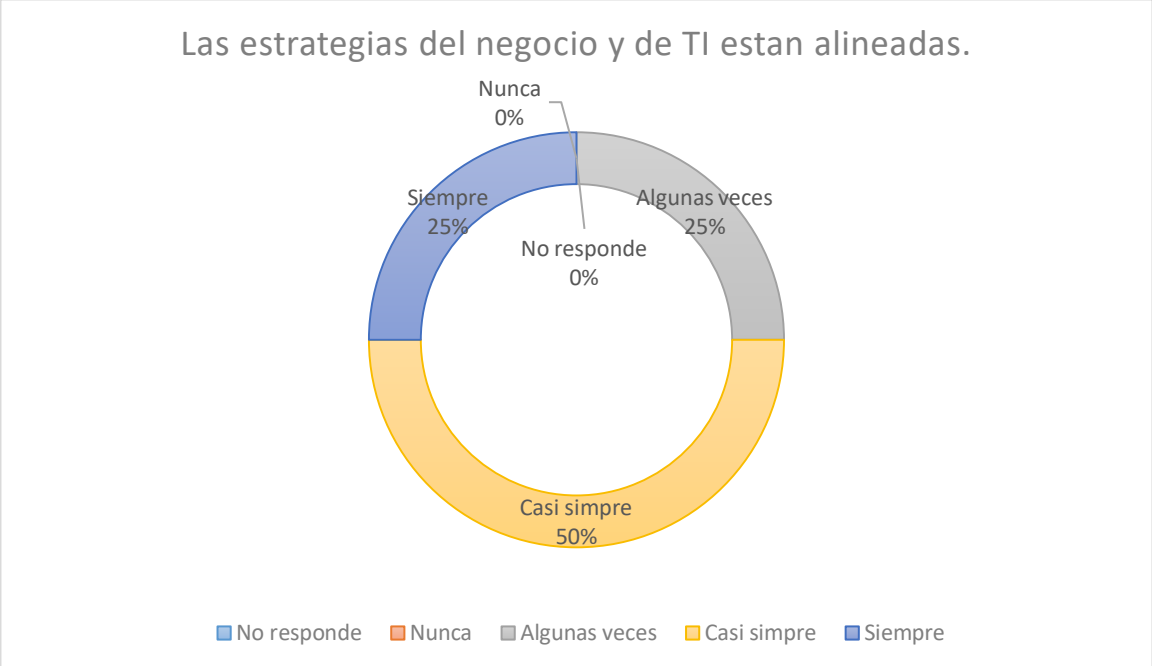
2.- Adquirir e implementar soluciones.

3.- Entregar y dar soporte

4.- Monitorear y evaluar

1.1 DOMINIO: PLANEAR Y ORGANIZAR

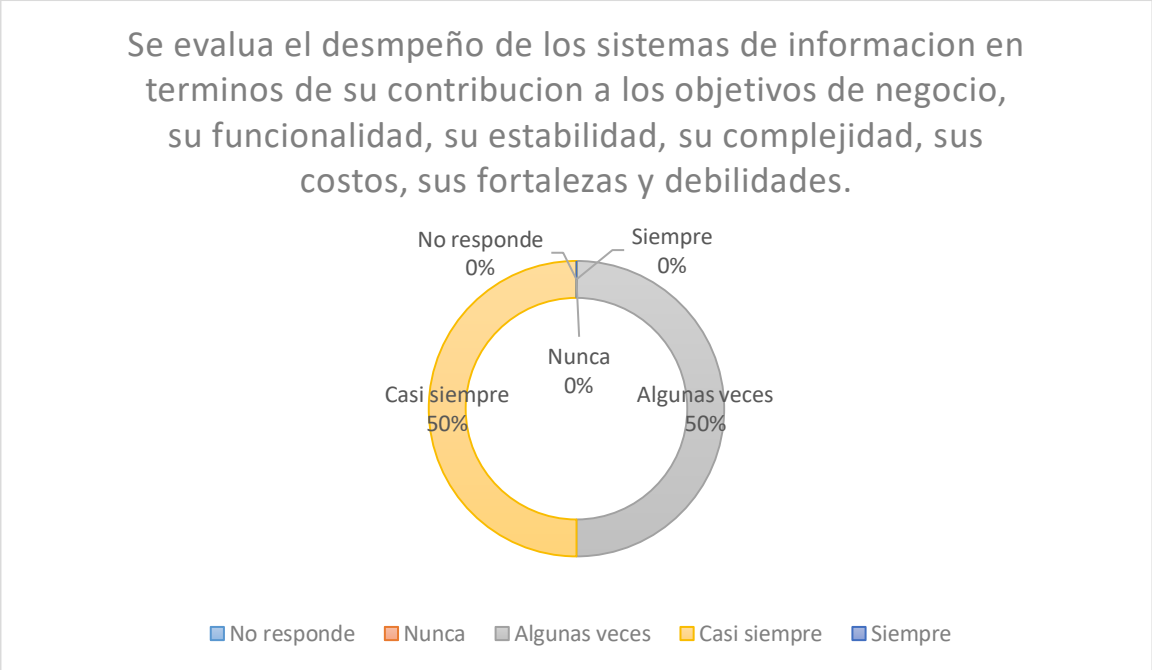
GRAFICO 1



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas encuestadas tienen alineadas las estrategias del negocio y de TI porque así ayuda a que la toma de decisiones vaya en directo beneficio de la organización, mientras que en partes iguales se encuentra algunas veces y casi siempre reflejando la importancia que dan a alinear las estrategias del negocio.

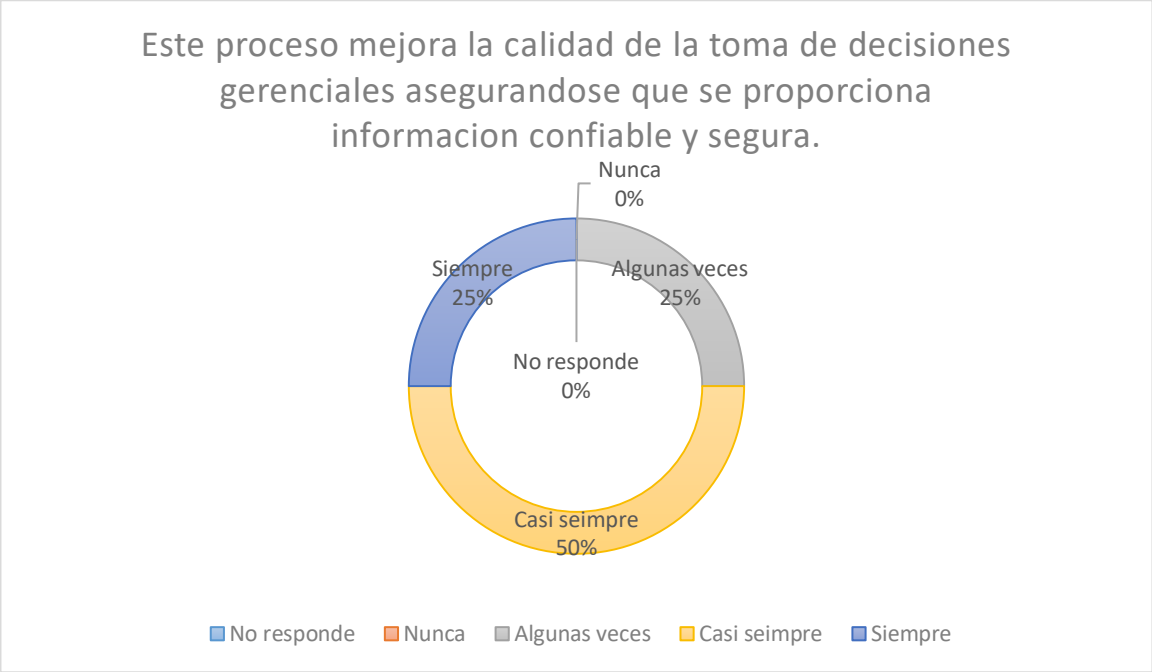
GRAFICO 2



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas casi siempre evalúa todo lo que conlleva tener un sistema de información siendo muy importante tener claro cada uno de sus aportes a la empresa, mientras que la otra mitad encuestada solo algunas veces evalúa el desempeño de los sistemas.

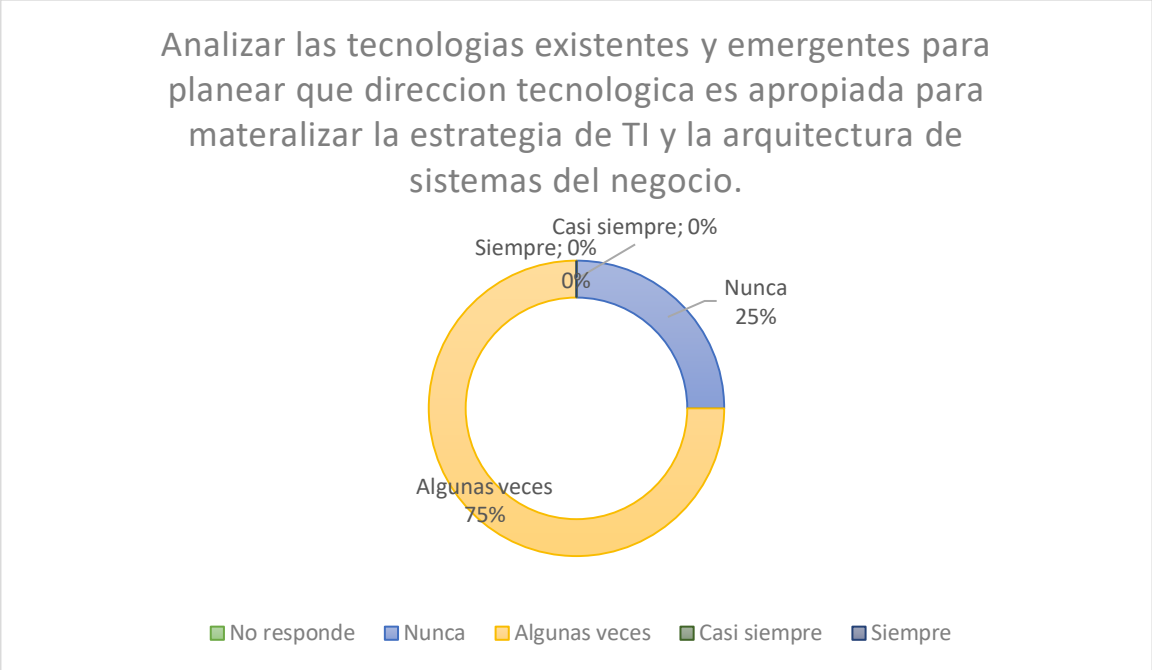
GRAFICO 3



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas encuestadas si toma este proceso como de importancia para la toma de decisiones, mientras mientras que el 25% algunas veces están conscientes de esto y el otro 25% siempre ha tomado consciencia de esto para el apoyo de la empresa.

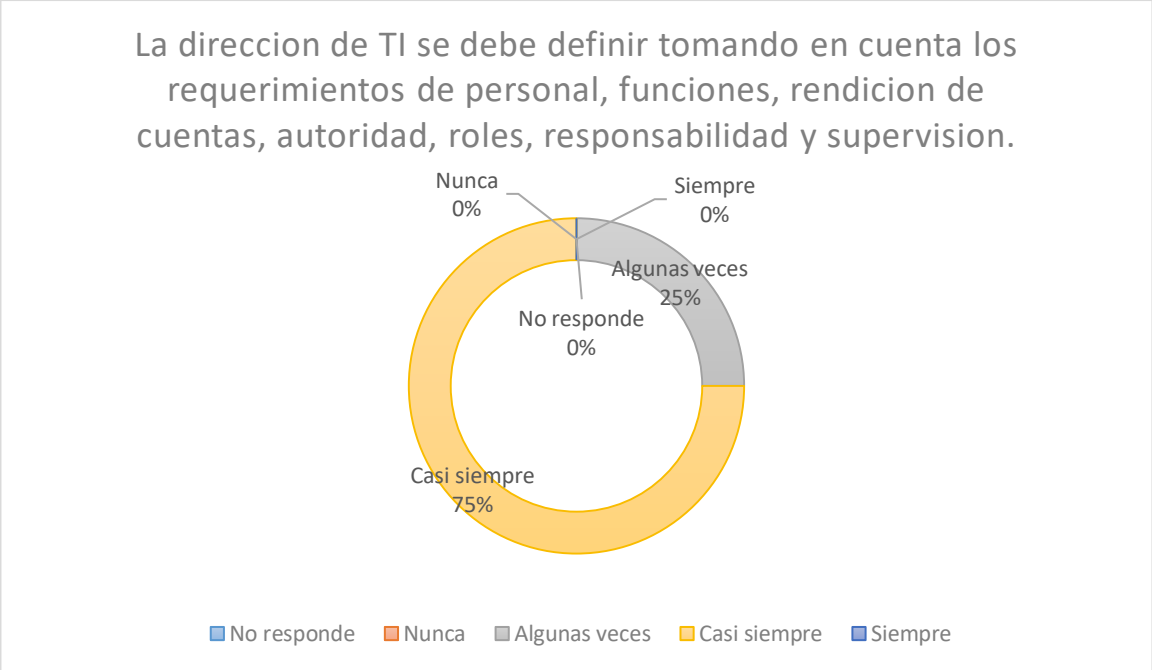
GRAFICO 4



Fuente aplicada a PYMES concepción, 2016

La mayoría de las empresas encuestadas si analizan y están conscientes de lo importante que es planear la dirección tecnológica apropiada así ayuda a conseguir la estrategia de TI, mientras que solo un 20% no analiza ni busca analizar las tecnologías existentes o las futuras.

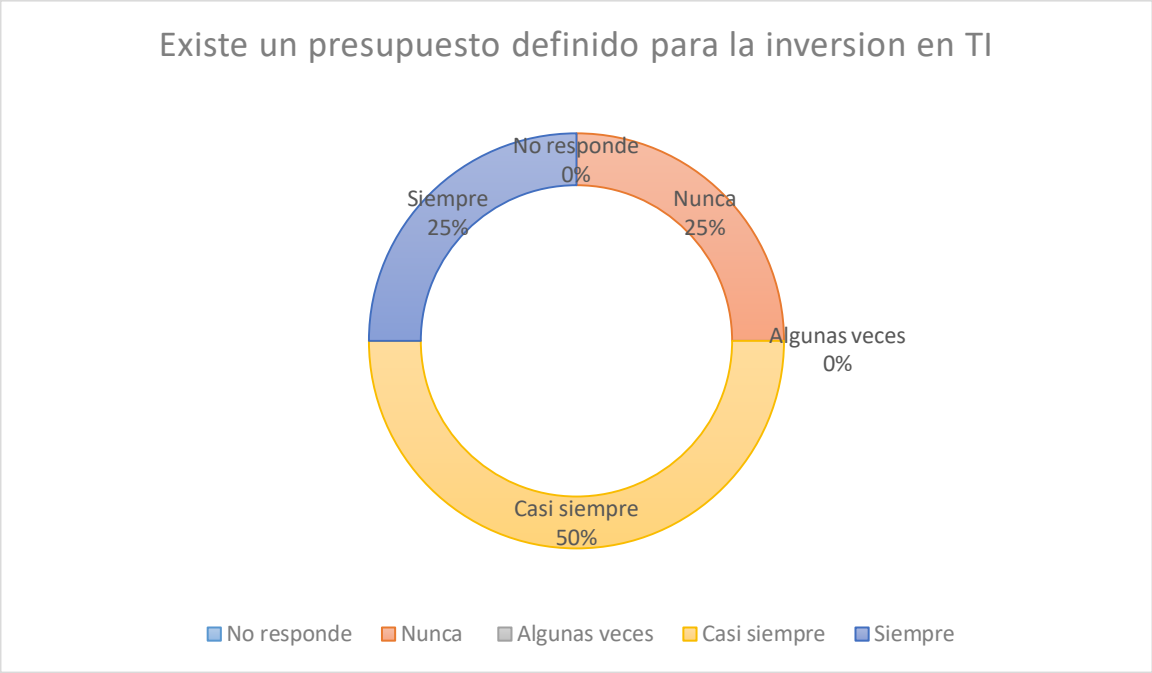
GRAFICO 5



Fuente aplicada a PYMES concepción, 2016

La gran mayoría de las empresas considera que la dirección de TI se debe definir tomando en cuenta todo lo que abarca, mientras que el restante solo algunas veces lo considera.

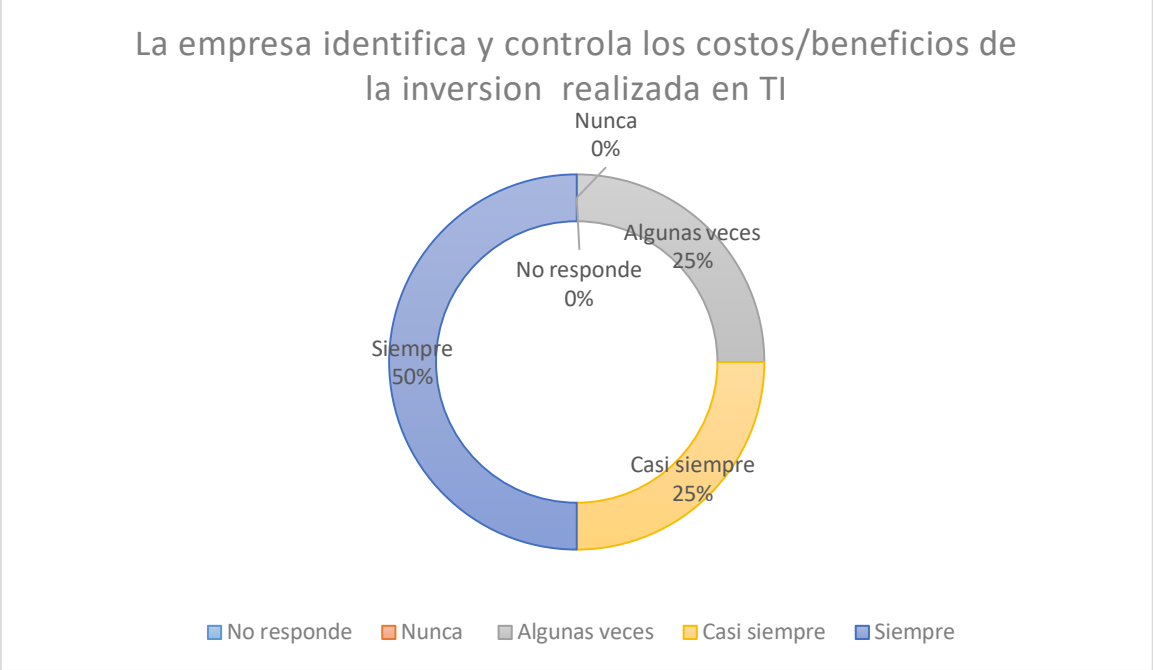
GRAFICO 6



Fuente aplicada a PYMES concepción, 2016

En la mitad de las Pymes encuestadas casi siempre existe un presupuesto para la inversión TI lo cual demuestra la constante preocupación de la gerencia, mientras que el 25% siempre existe una inversión destinada a TI y en el último caso nunca ha existido demostrando completa despreocupación por parte de dueños, gerencia o quien tome las decisiones dentro de la empresa.

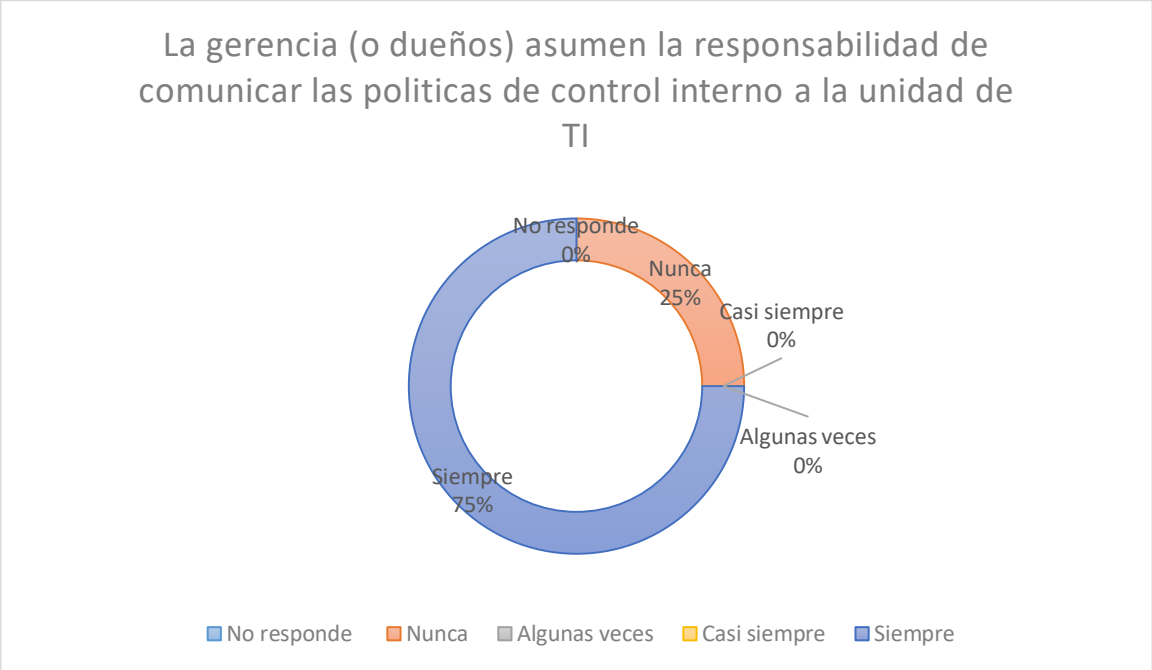
GRAFICO 7



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas siempre controla los costos/beneficios asociados a la inversión TI, mientras que dividido en partes iguales casi siempre 25% y algunas veces 25% controla estos costos/beneficios.

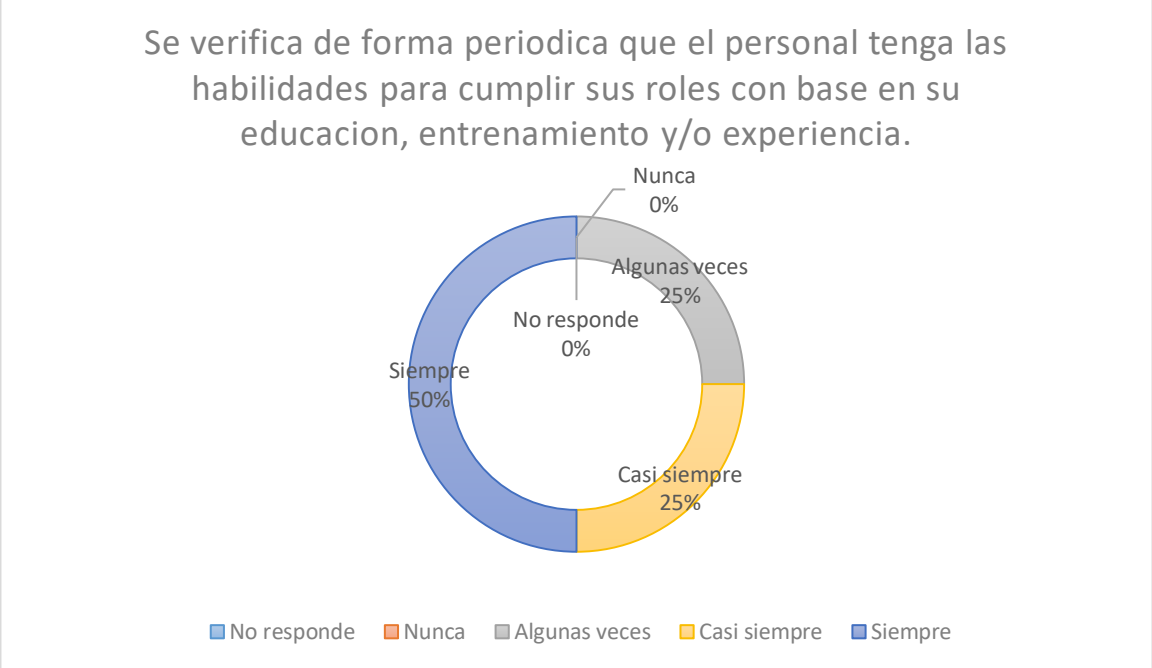
GRAFICO 8



Fuente aplicada a PYMES concepción, 2016

La gran mayoría de las empresas está de acuerdo con ser ellas las encargadas de comunicar las políticas de control interno a todas las unidades para que no existan confusiones o acciones que puedan perjudicar a la organización, mientras que el 25% restante nunca considera como opción informar las políticas de cada unidad.

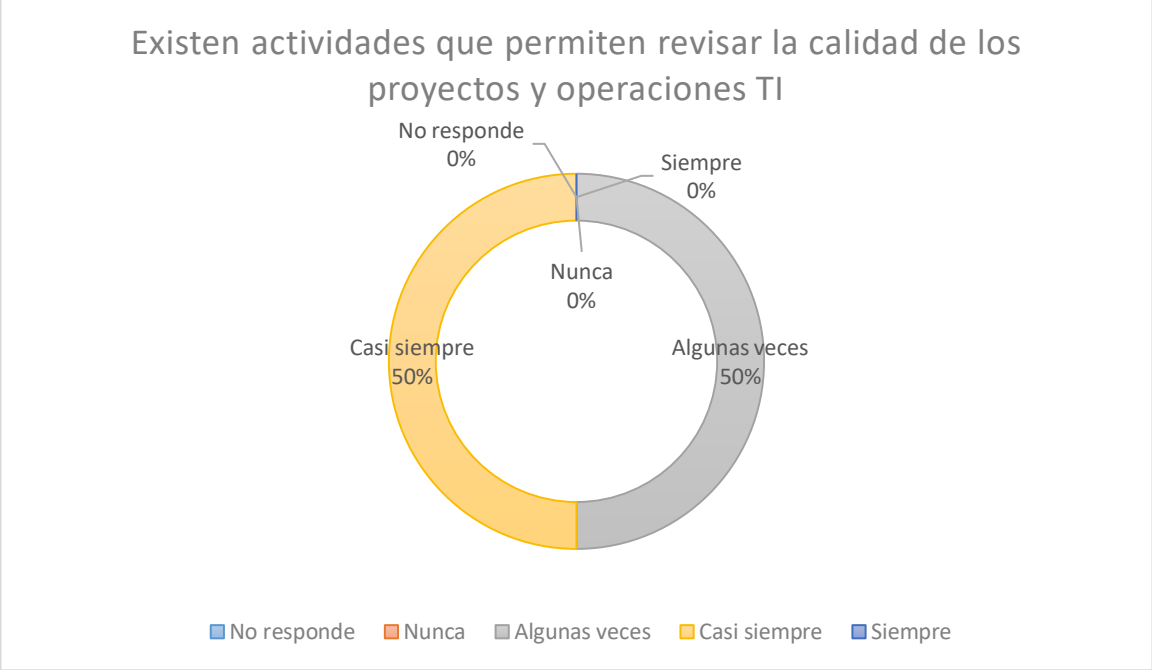
GRAFICO 9



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas consideran la verificación del personal para que cumplan con el trabajo encomendado, mientras tanto casi siempre se hace la revisión y algunas veces no se llegan a concretar.

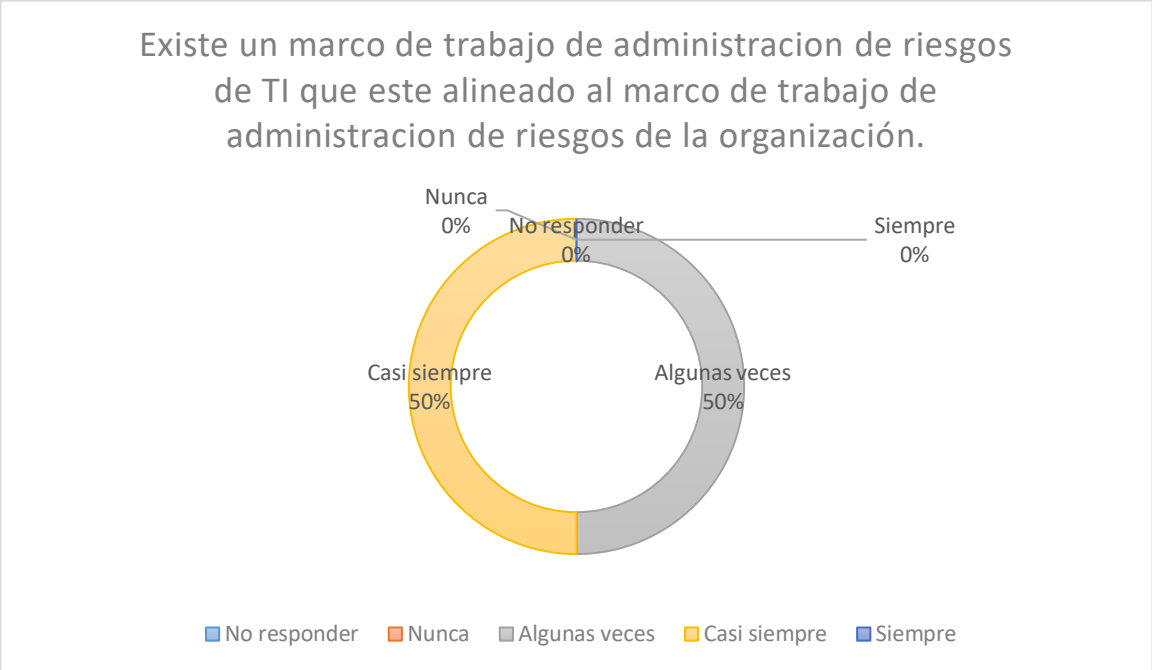
GRAFICO 10



Fuente aplicada a PYMES concepción, 2016

Repartido en partes iguales las empresas revisan la calidad de los proyectos y operaciones TI casi siempre, mientras que la otra mitad lo hace algunas veces.

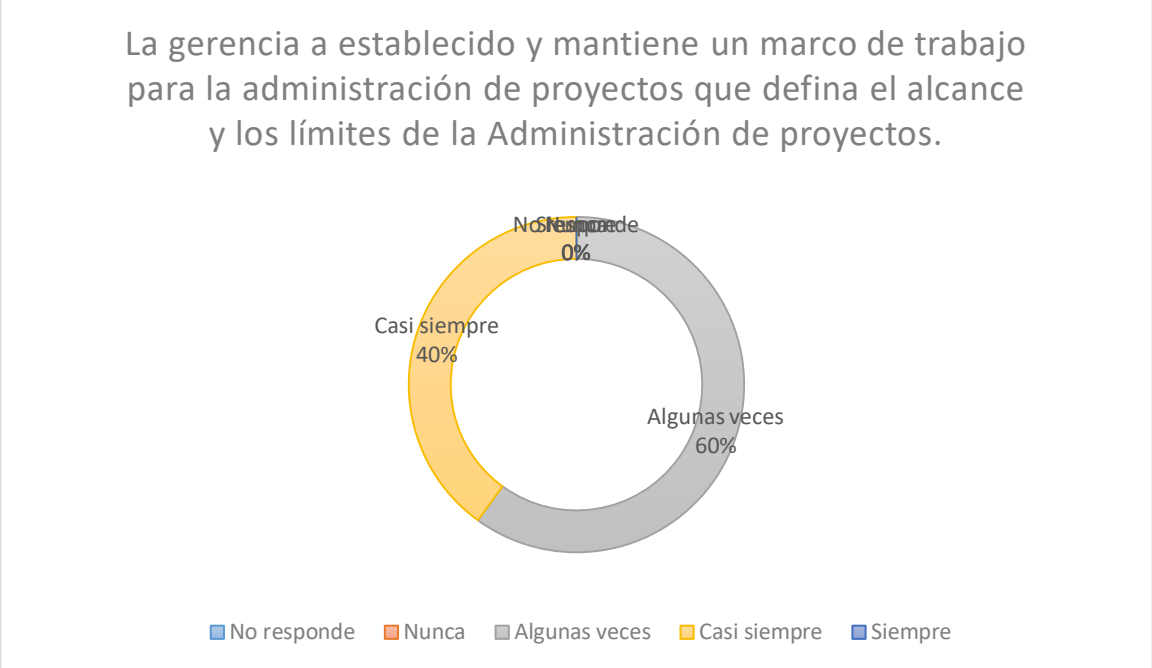
GRAFICO 11



Fuente aplicada a PYMES concepción, 2016

En la mitad de las empresas si existe casi siempre un marco de trabajo de administración de riesgos de TI, mientras que en la otra mitad solo algunas veces existe.

GRAFICO 12

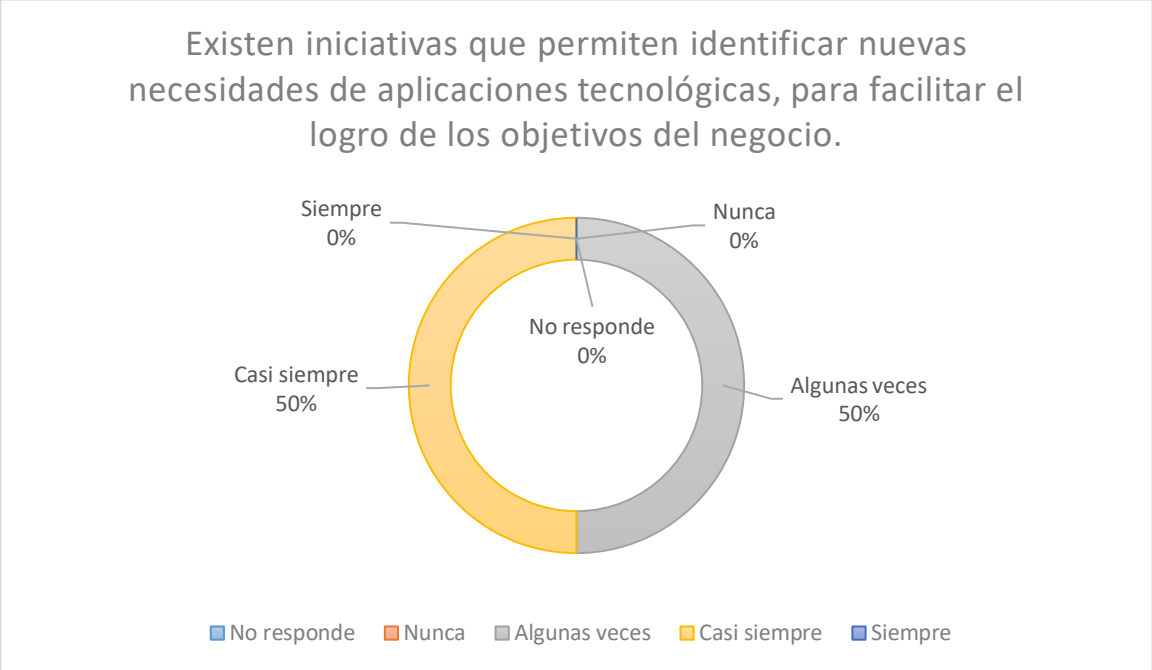


Fuente aplicada a PYMES concepción, 2016

De las empresas encuestadas poca más de la mitad solo algunas veces ha establecido un marco de trabajo para la administración de proyectos, mientras que el restante solo casi siempre existe un marco de trabajo para la administración de proyectos.

1.2 DOMINIO DE ADQUIRIR E IMPLEMENTAR

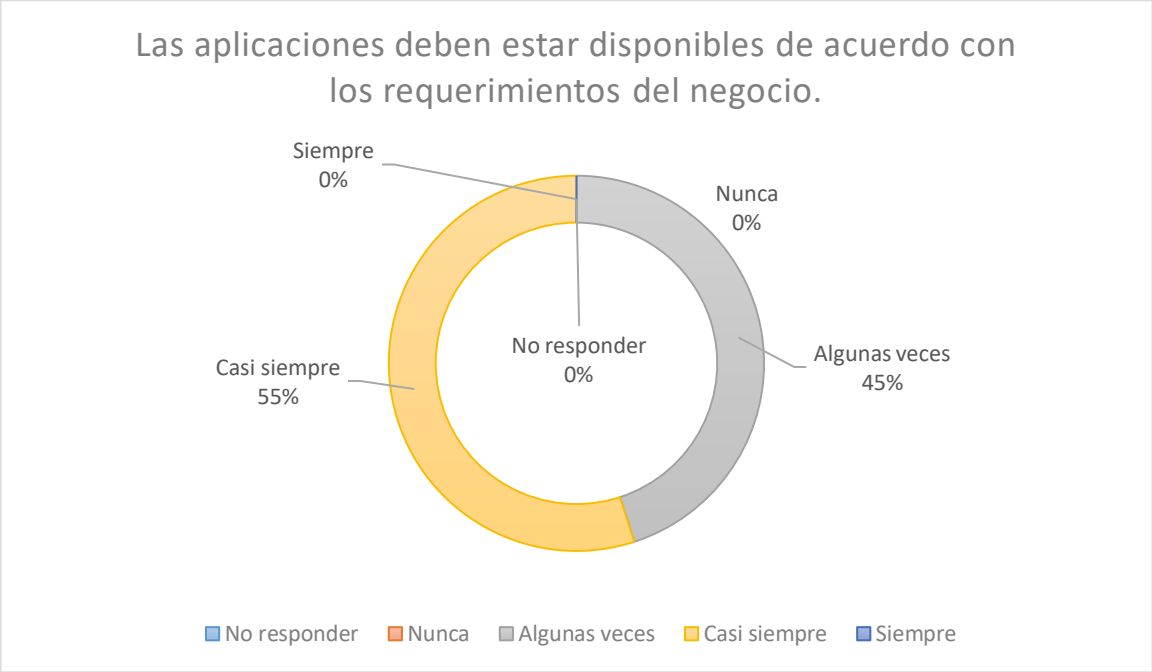
GRAFICO 13



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas solo algunas veces se preocupa de identificar nuevas necesidades de tecnologías, mientras que la otra mita casi siempre existen iniciativas

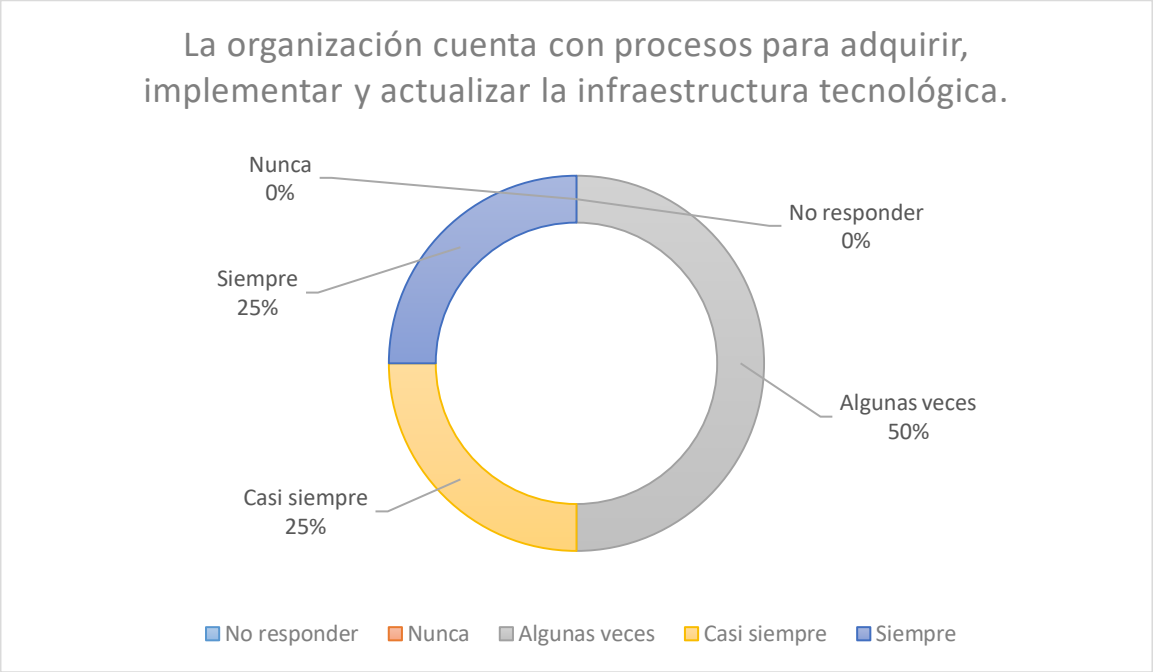
GRAFICO 14



Fuente aplicada a PYMES concepción, 2016

Casi la gran mayoría de las empresas las aplicaciones deben estar disponibles los requerimientos del negocio, mientras que el restante solo algunas veces está disponible.

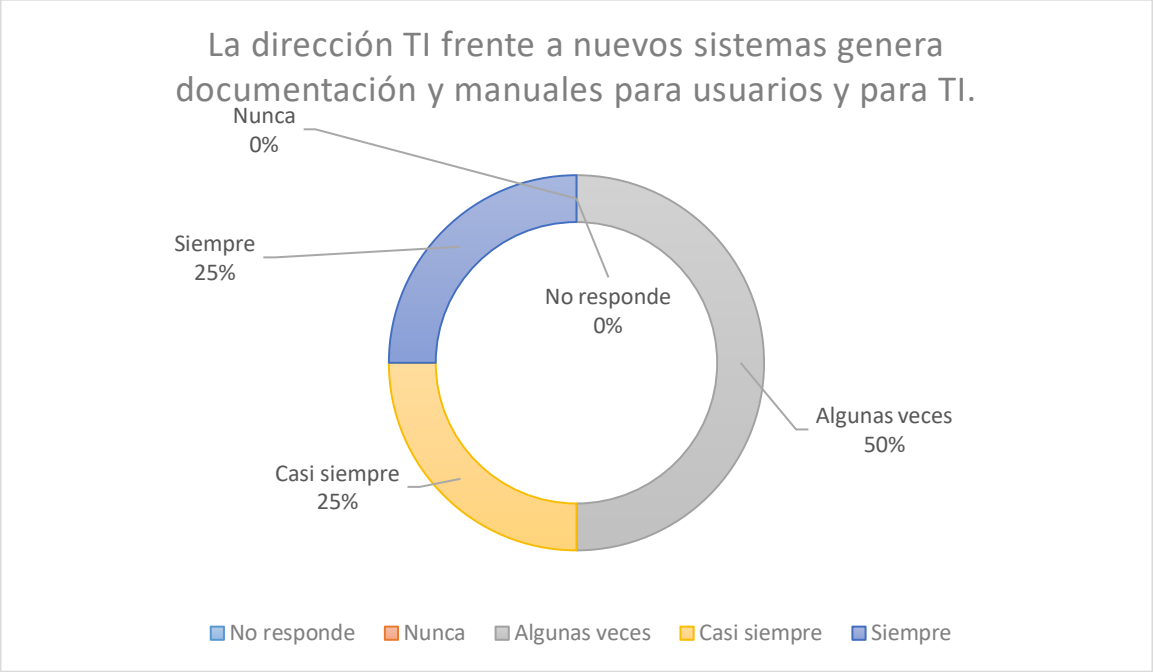
GRAFICO 15



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas cuenta con procesos para adquirir, implementar y actualizar la estructura tecnológica, mientras que en partes iguales siempre y casi siempre existen procesos.

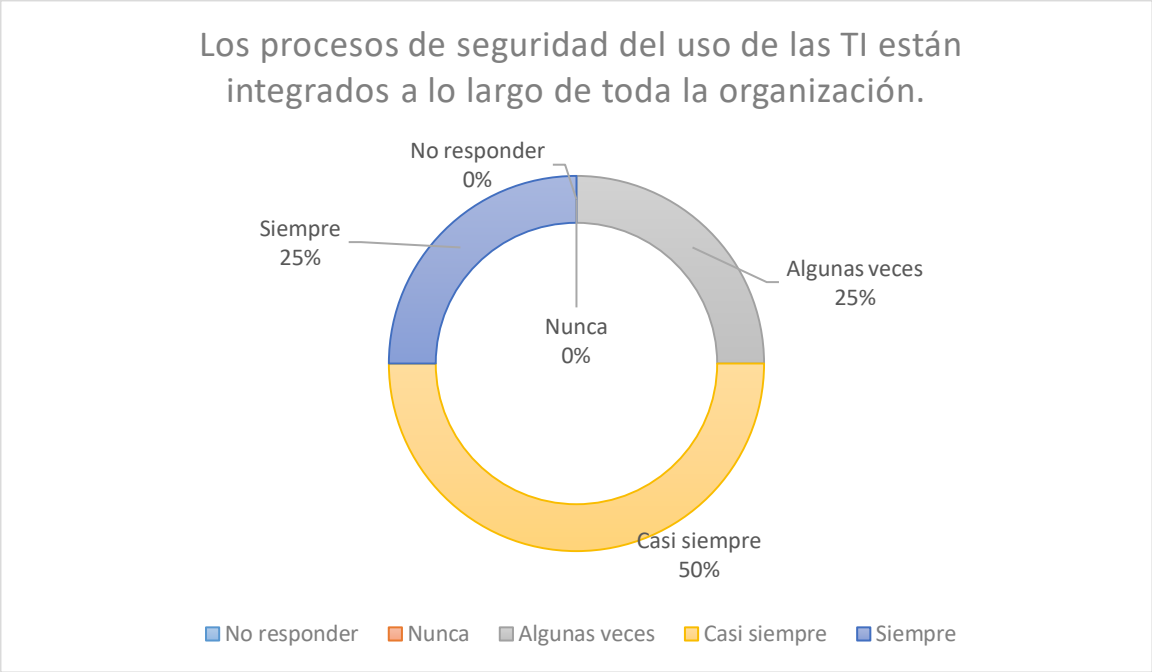
GRAFICO 16



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas algunas veces generan anuales frente a nuevos sistemas, mientras que en igual cantidad siempre y casi siempre existen.

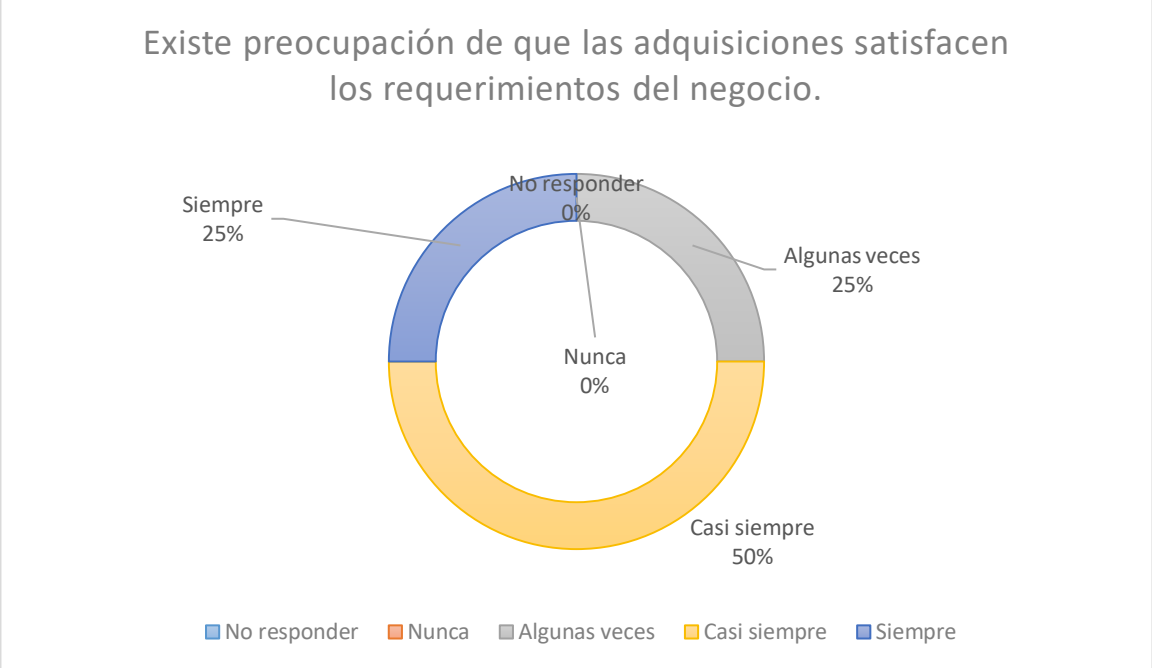
GRAFICO 17



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas contesto que casi siempre todos los procesos de seguridad están integrados, mientras que en partes iguales se encuentran siempre y algunas veces.

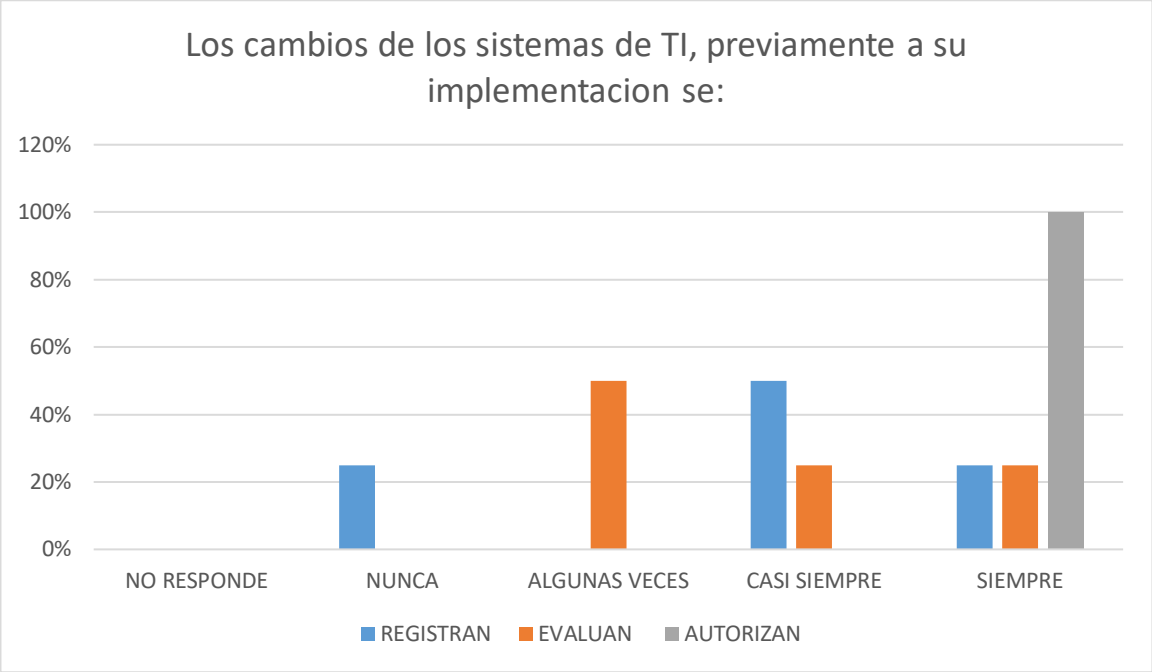
GRAFICO 18



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas casi siempre están preocupados de las adquisiciones y que vayan en directo beneficio de la organización, mientras que en partes iguales se encuentran siempre y algunas veces.

GRAFICO 19

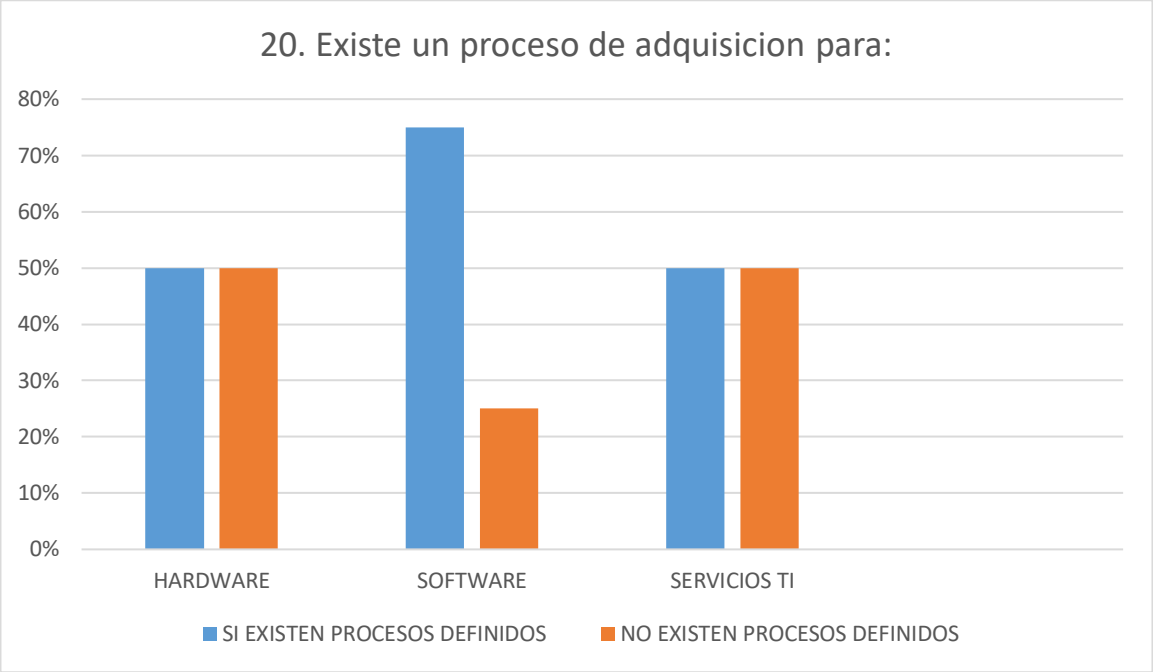


Fuente aplicada a PYMES concepción, 2016

Las empresas encuestadas para la implementación de cambios en los sistemas de TI en general se registran, se evalúan y posteriormente el 100% de las empresas pasan por la autorización de la gerencia o encargados del negocio.

Con lo expuesto se expresan las falencias que se encuentran en el registro de los cambios y la evaluación en ocasiones se pasa por alto pero el punto en donde todos los negocios concuerdan es en la autorización que siempre debe existir por parte de los encargados de administrar la empresa.

GRAFICO 20

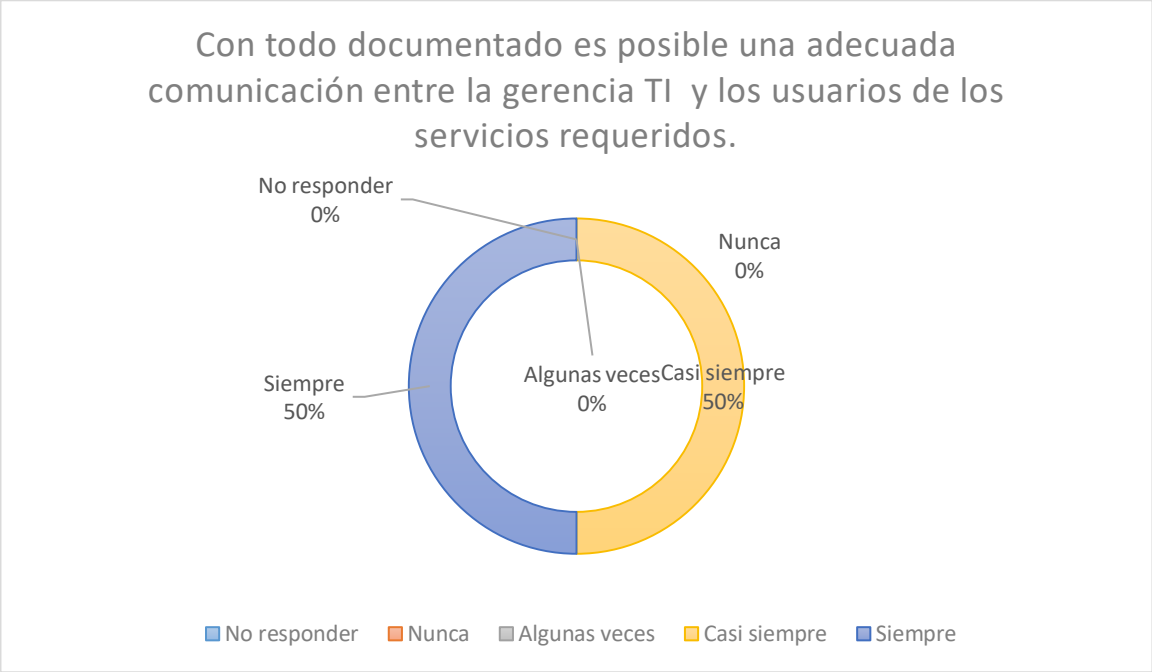


Fuente aplicada a PYMES concepción, 2016

Se puede ver que a veces existen procesos para adquirir e implementar soluciones TI, muchas veces solo se preocupan cuando hay fallas que afecta la realización de las tareas de la empresa sin consideran procesos más continuos de revisión que ayuden a renovar productos antes de que exista fallas.

1.3 DOMINIO DE ENTREGAR Y DAR SOPORTE

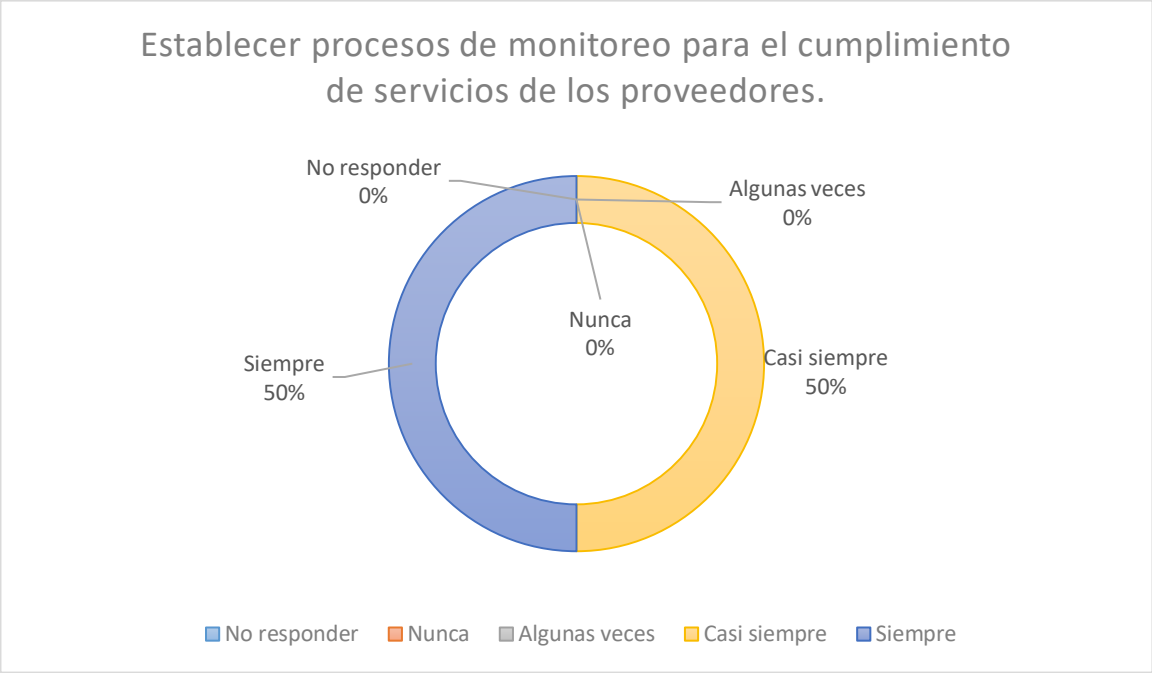
GRAFICO 21



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas consideran siempre que con todo documentado es posible una buena comunicación entre la gerencia de TI y quien utiliza los servicios, mientras que la otra mitad considera que casi siempre esto se puede lograr.

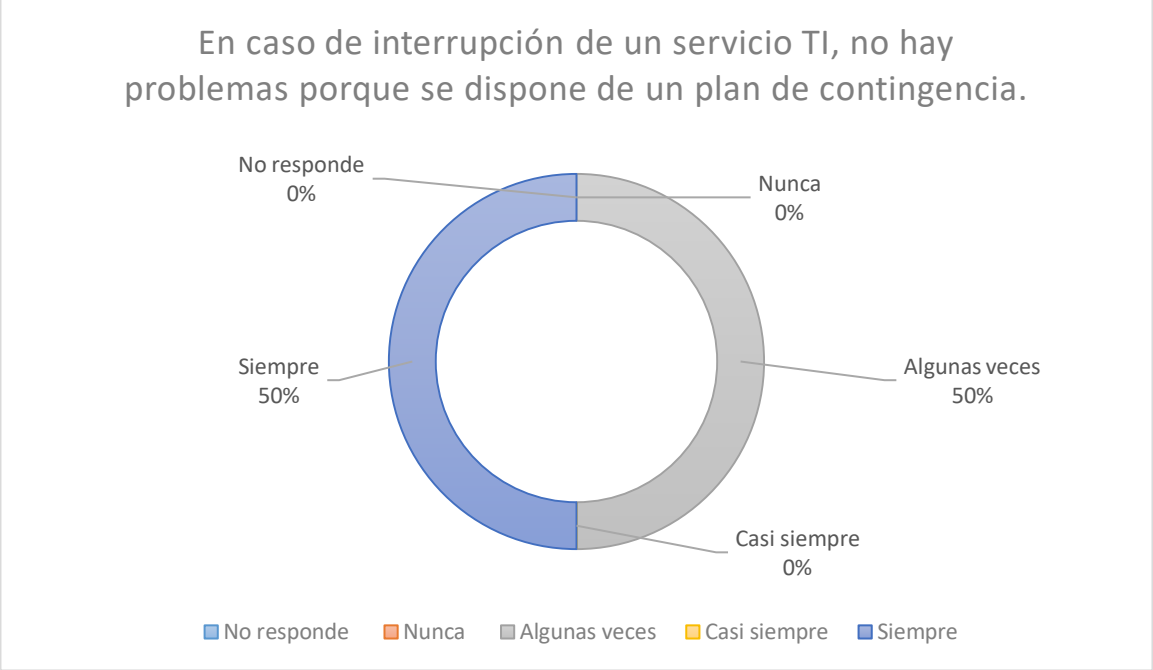
GRAFICO 22



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas establece algún control para el cumplimiento de los servicios de los proveedores, mientras que la otra mitad casi siempre hace algún control.

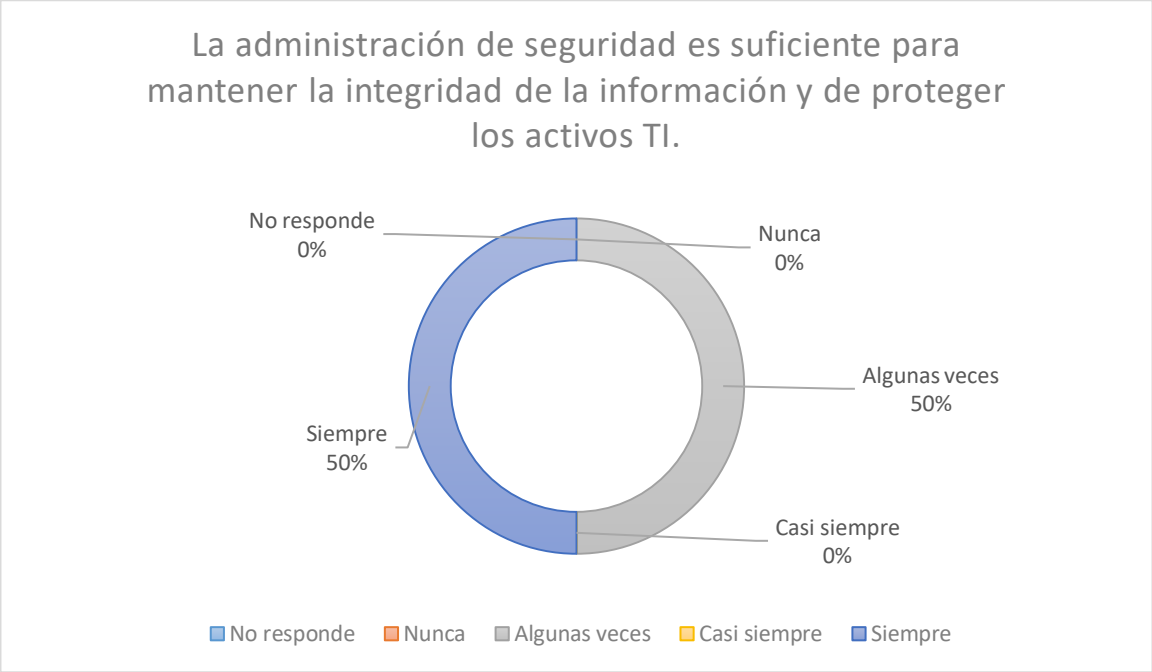
GRAFICO 23



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas dispone de un plan de contingencia, mientras que la otra mitad no la otra solo algunas veces dispone un plan.

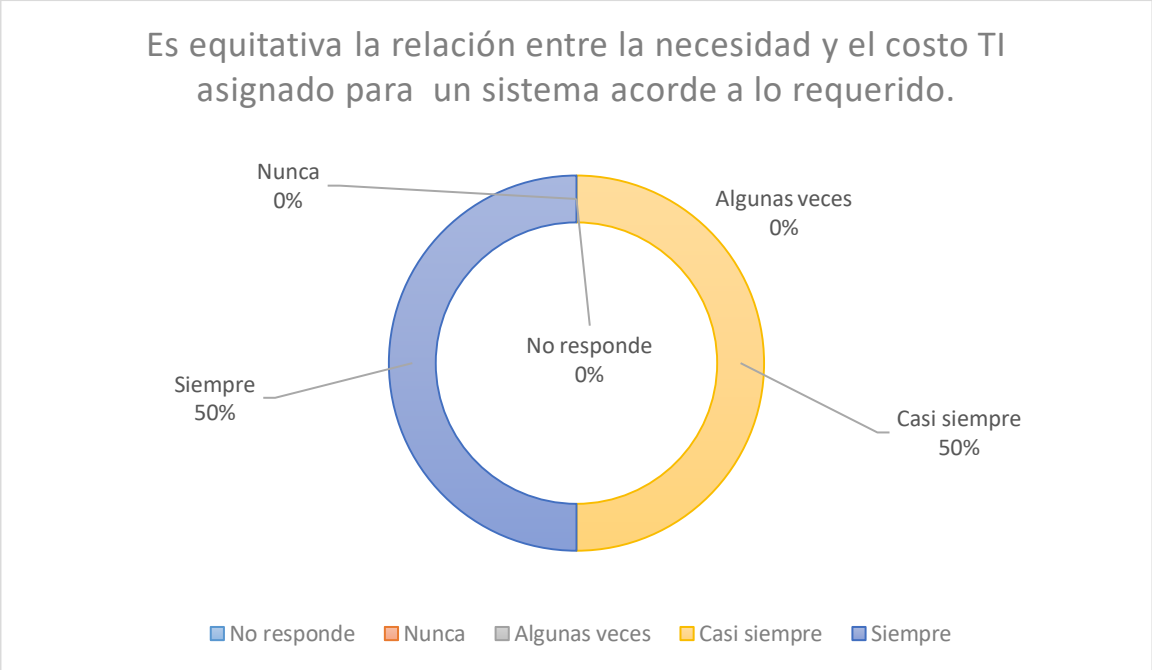
GRAFICO 24



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas consideran que es suficiente la administración de seguridad. Mientras que la otra mitad algunas veces considera que si es suficiente.

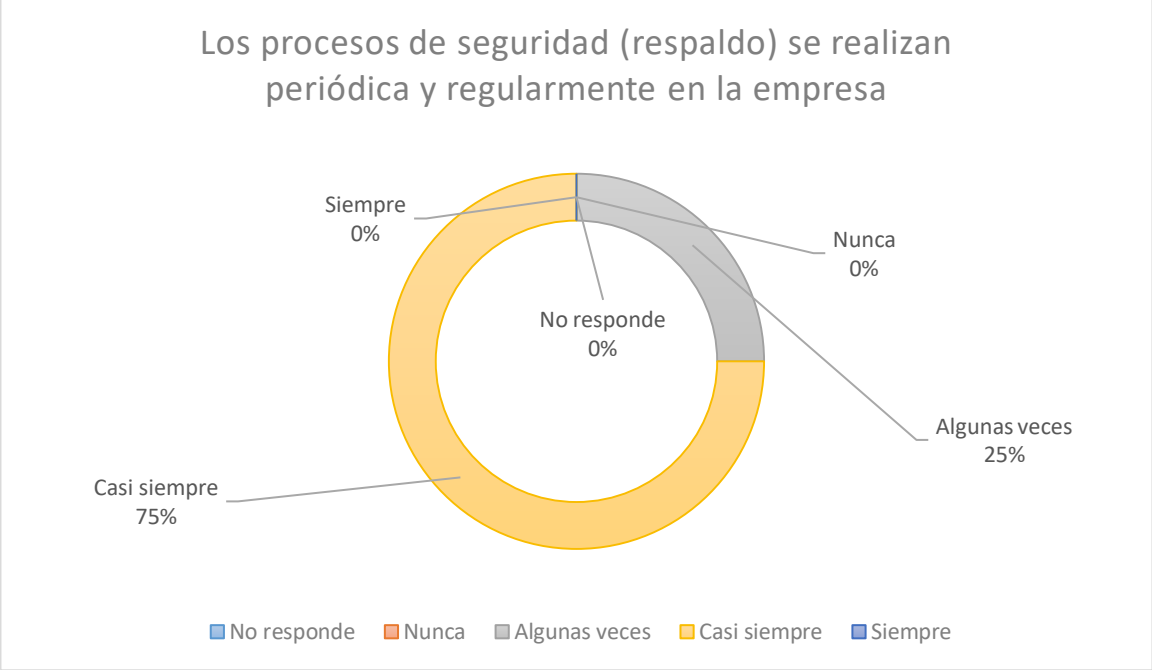
GRAFICO 25



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas siempre cree que la relación entre la necesidad y el costo TI asignado para un sistema es acorde a lo requerido, mientras que la otra mitad casi siempre considera equitativa la relación.

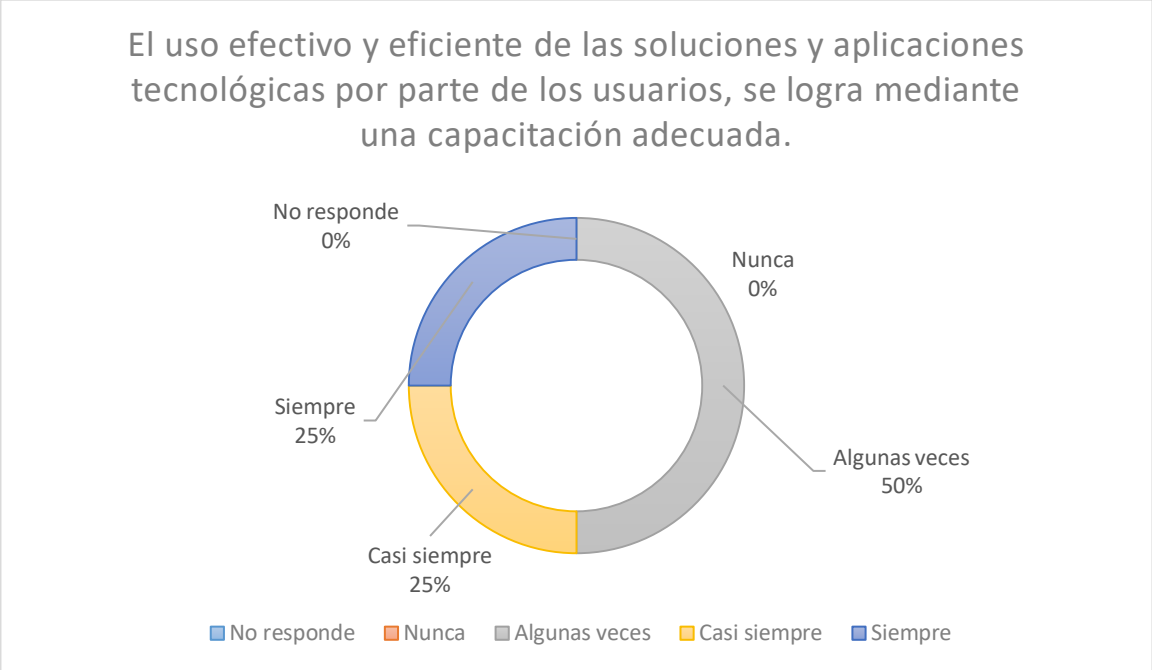
GRAFICO 26



Fuente aplicada a PYMES concepción, 2016

La mayoría de las empresas aseguran que los procesos de respaldo se realizan de forma periódica para tener una mayor seguridad, mientras que la cantidad restante dice que solo algunas veces se realizan procesos de respaldo periódicamente.

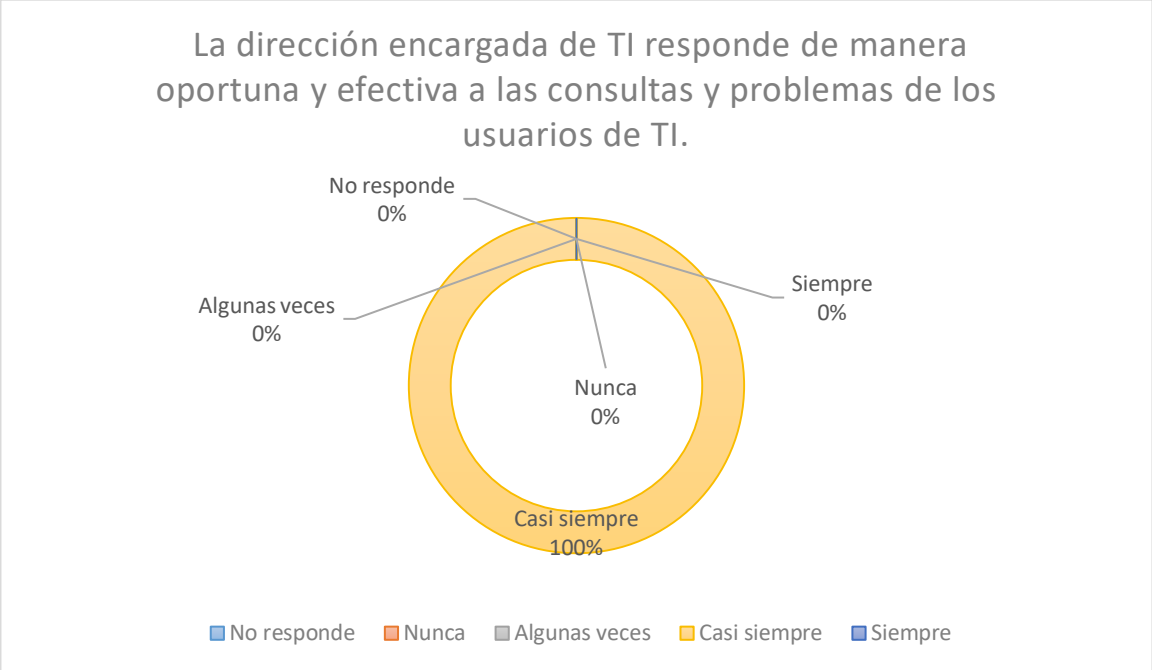
GRAFICO 27



Fuente aplicada a PYMES concepción, 2016

La mitad de las PYMES encuestadas algunas veces cree que la clara comprensión por parte de los usuarios se logra mediante una capacitación adecuada, mientras que en cantidades iguales siempre y casi siempre considera esto como efectivo.

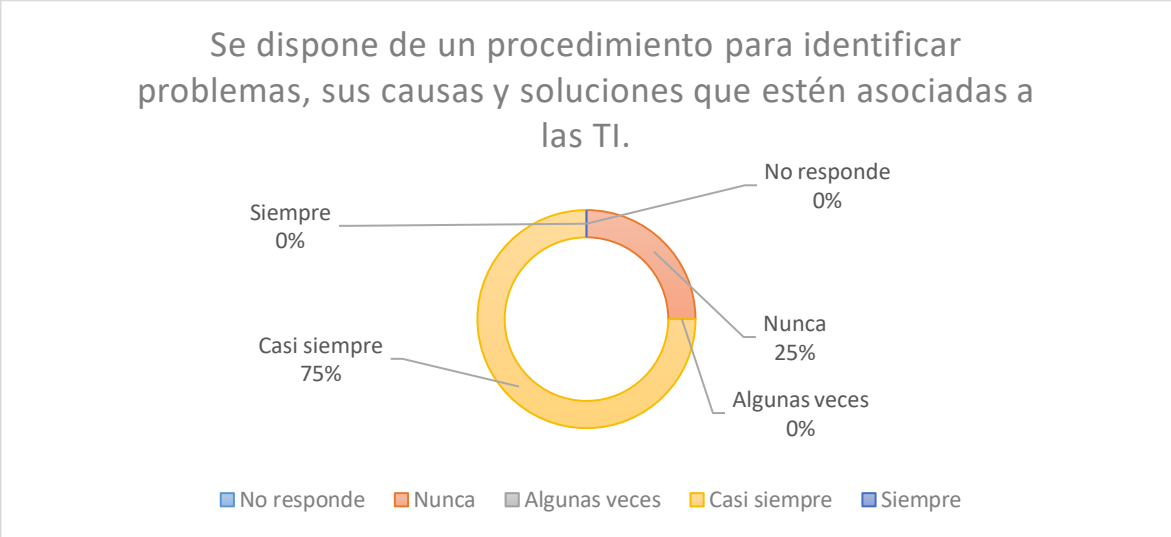
GRAFICO 28



Fuente aplicada a PYMES concepción, 2016

Todas las empresas creen que la dirección encargada de TI responde de manera oportuna y efectiva a las consultas generando confianza en el servicio entregado.

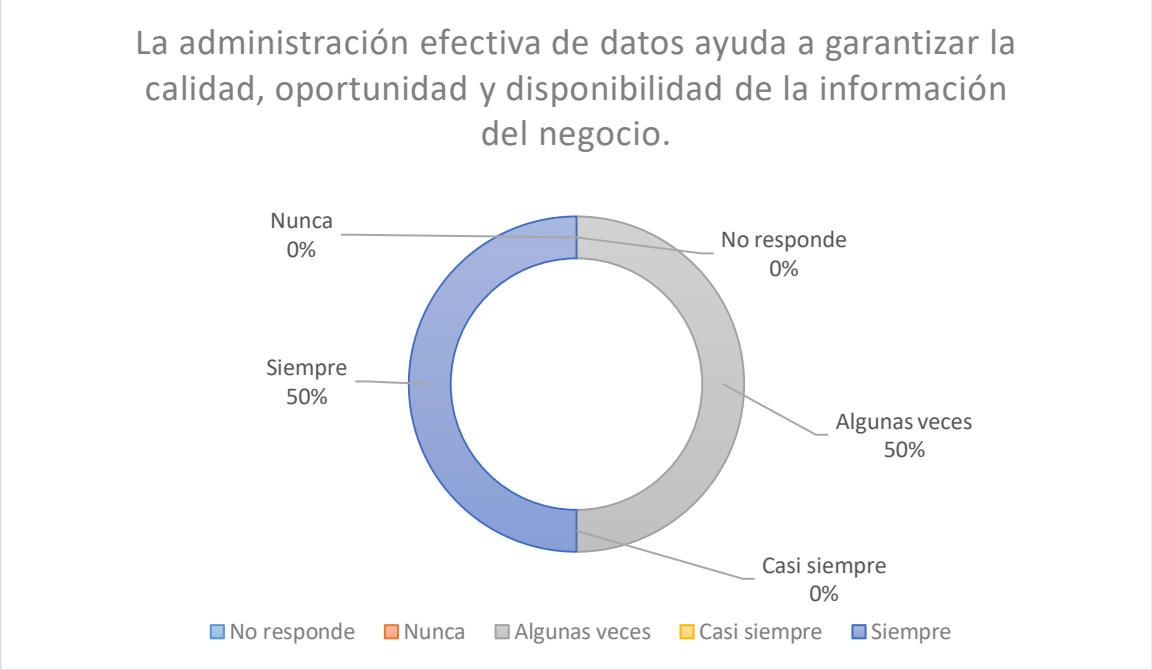
GRAFICO 29



Fuente aplicada a PYMES concepción, 2016

La mayoría de las empresas aseguran que disponen de un procedimiento para identificar problemas y soluciones todas asociadas a TI, mientras que la cantidad restante considera que nunca se ha tenido este procedimiento.

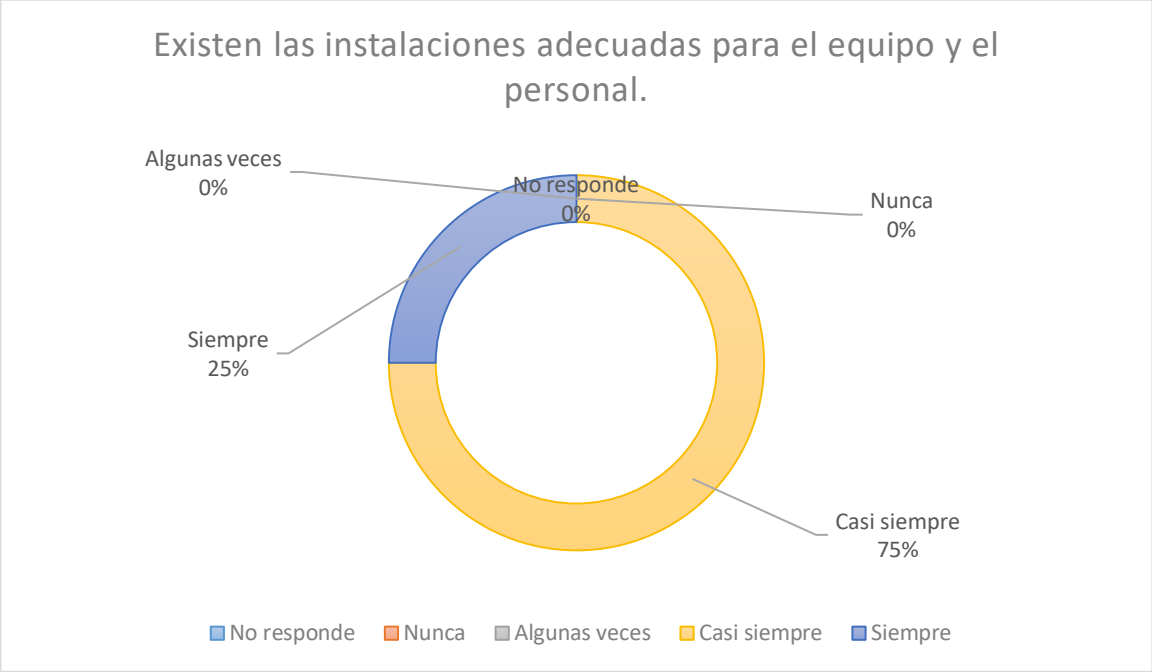
GRAFICO 30



Fuente aplicada a PYMES concepción, 2016

La mitad de empresas dice que una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio, mientras que la otra mitad dice que solo a veces es efectiva esta administración.

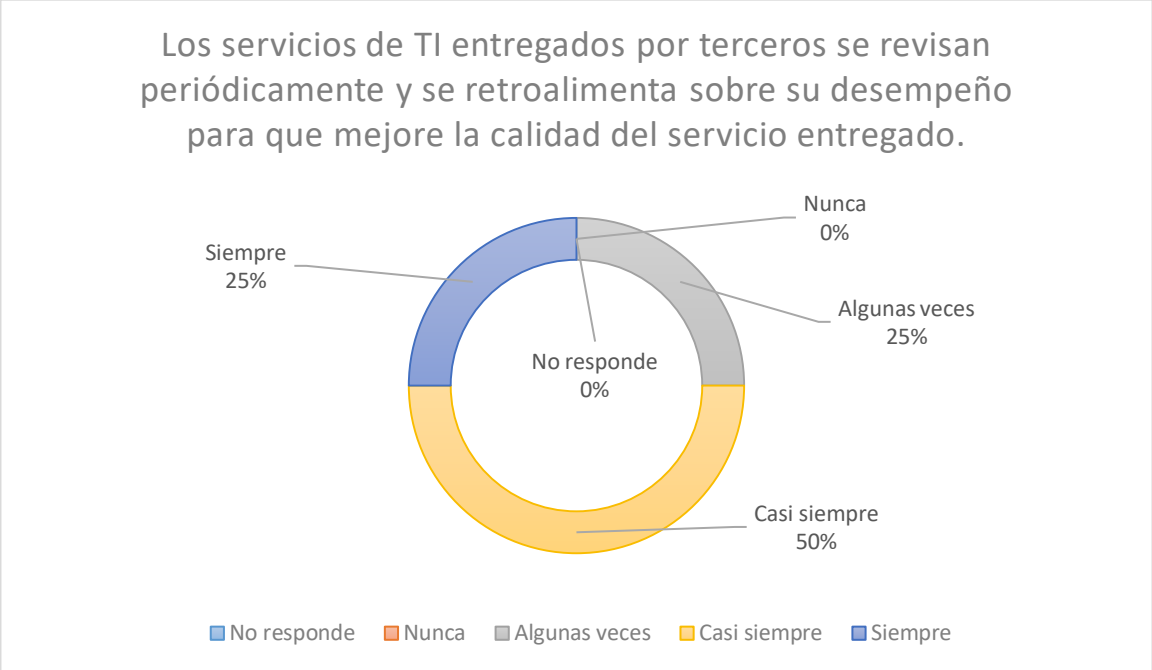
GRAFICO 31



Fuente aplicada a PYMES concepción, 2016

La mayoría de las empresas dice asegurar que existen las instalaciones adecuadas para el equipo y el personal, mientras que la cantidad restante asegura que siempre existen.

GRAFICO 32

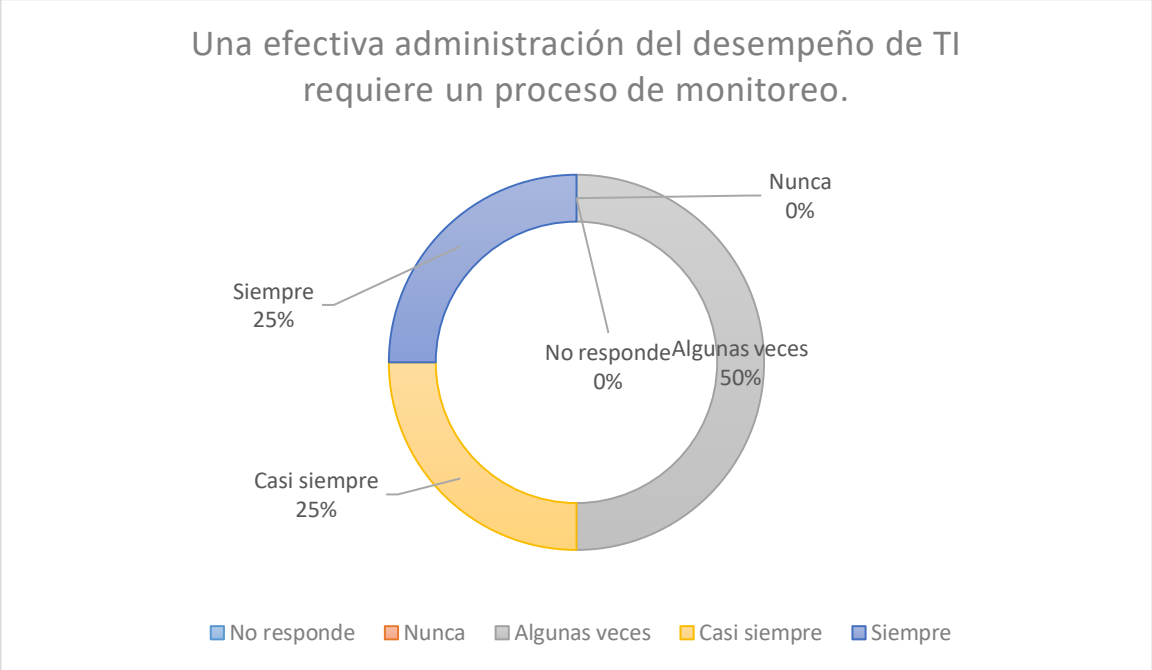


Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas aseguran que casi siempre los servicios TI entregados por terceros son revisados periódicamente, mientras que en partes iguales la cantidad restante siempre o algunas veces se revisan periódicamente la calidad de los servicios entregados.

1.4 DOMINIO DE MONITOREAR Y EVALAUR

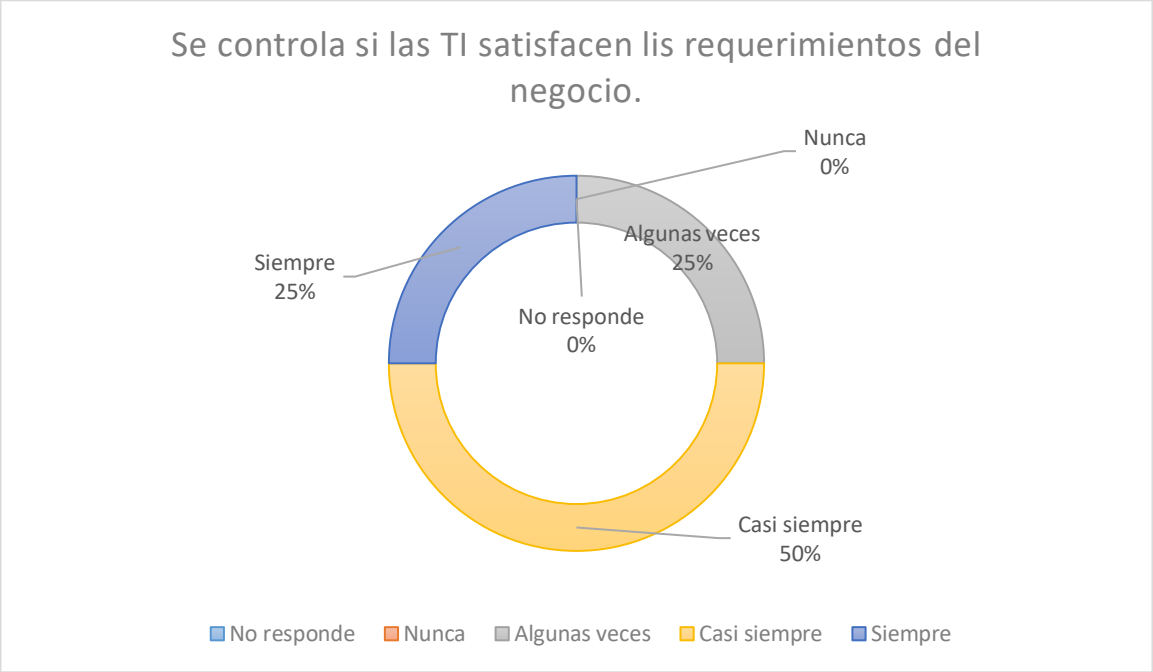
GRAFICO 33



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas afirma que algunas veces se monitorea el desempeño TI, mientras que en cantidades iguales casi siempre y siempre se realiza el monitoreo del desempeño de TI.

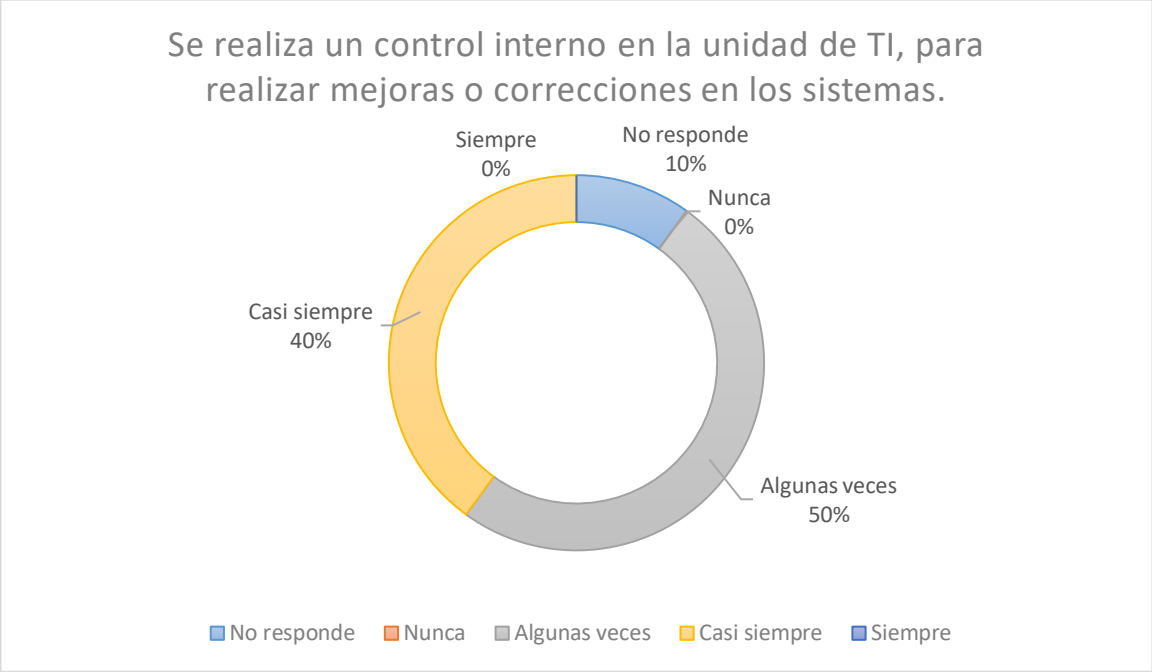
GRAFICO 34



Fuente aplicada a PYMES concepción, 2016

Las mitad de las empresas casi siempre controla que las TI satisfáganlos requerimientos del negocio, mientras que igual cantidad siempre o algunas veces no se controla las TI.

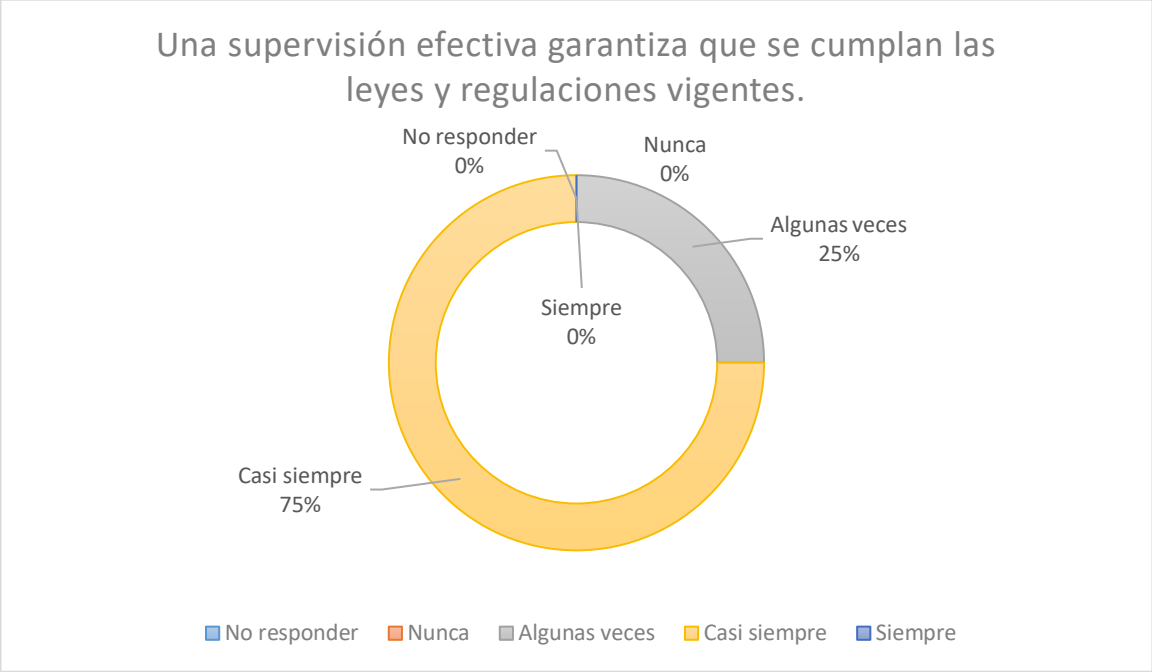
GRAFICO 35



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas algunas veces realiza un control interno en la unidad TI para realizar mejoras, mientras que un 40% afirma que casi siempre lo hace mientras que el 10% restante no responde a la pregunta.

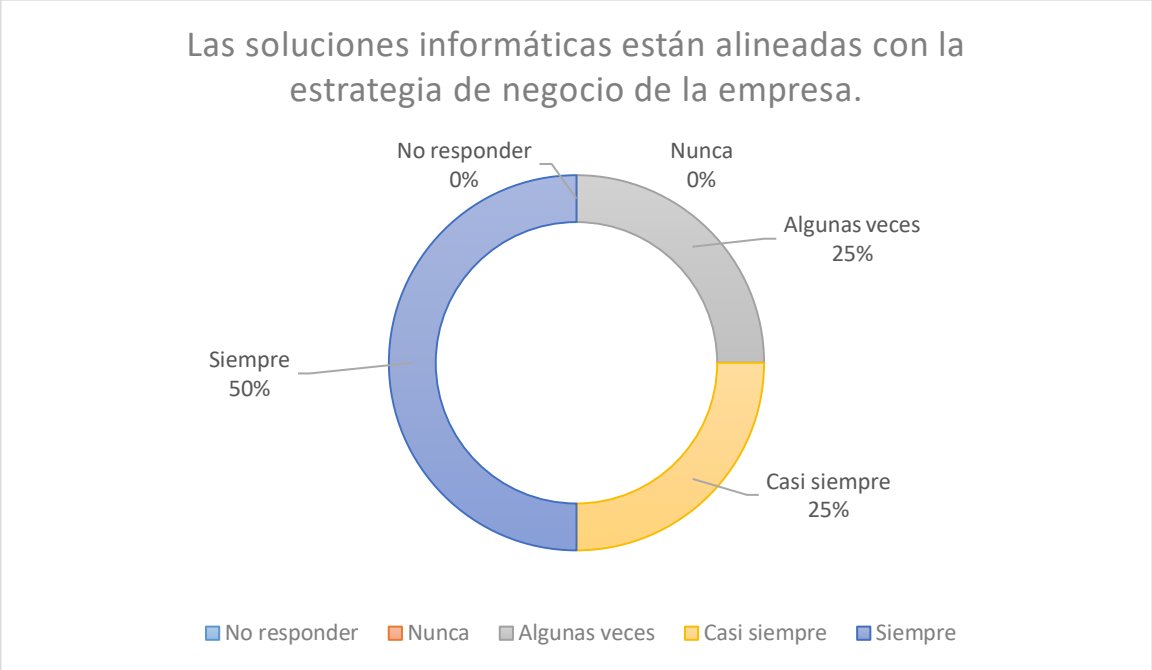
GRAFICO 36



Fuente aplicada a PYMES concepción, 2016

La mayoría de las empresas a través de la supervisión efectiva garantiza cumplir las leyes y regulaciones, mientras que 25% solo algunas veces realiza una supervisión.

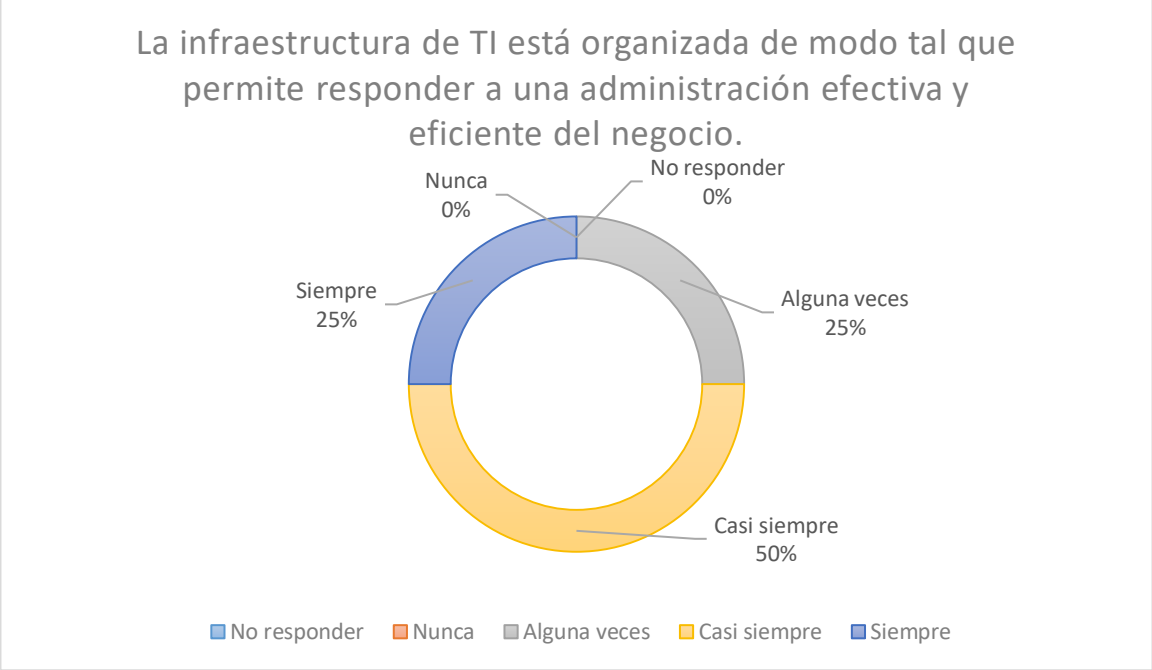
GRAFICO 37



Fuente aplicada a PYMES concepción, 2016

La mitad de las empresas aseguran que las soluciones informáticas están alineadas con la estrategia del negocio, mientras que en igual forma un 25% casi siempre y un 25% alguna vez aseguras que las soluciones están alienadas.

GRAFICO 38



Fuente aplicada a PYMES concepción, 2016

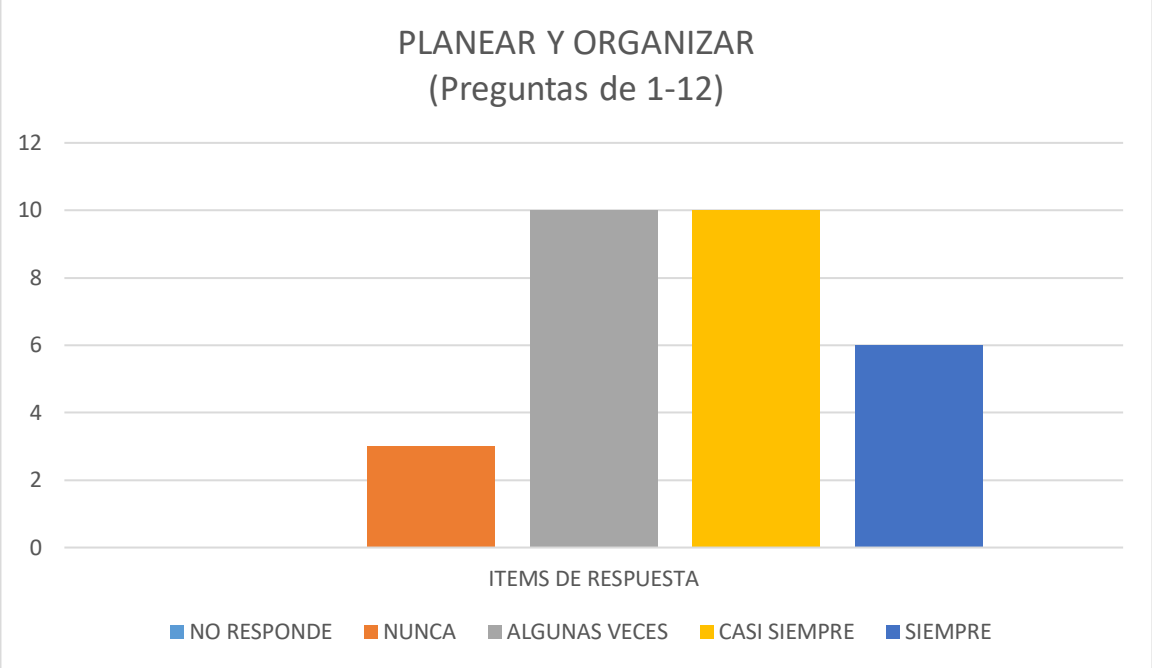
La mitad de las empresas aseguran que la infraestructura de TI permite responder a una administración efectiva y eficiente del negocio, mientras que un 25% siempre ha visto que la infraestructura de TI permite una buena administración y el 25% restante dice que solo algunas veces ha notado esto

OBSERVACIONES

Se analizan los resultados obtenidos de las empresas PYMES encuestadas para saber cuál es la situación actual en la que se encuentran frente a la seguridad de información que tienen implantada dentro de cada organización.

PLANEAR Y ORGANIZAR

Resultados obtenidos por cada dominio a continuación:

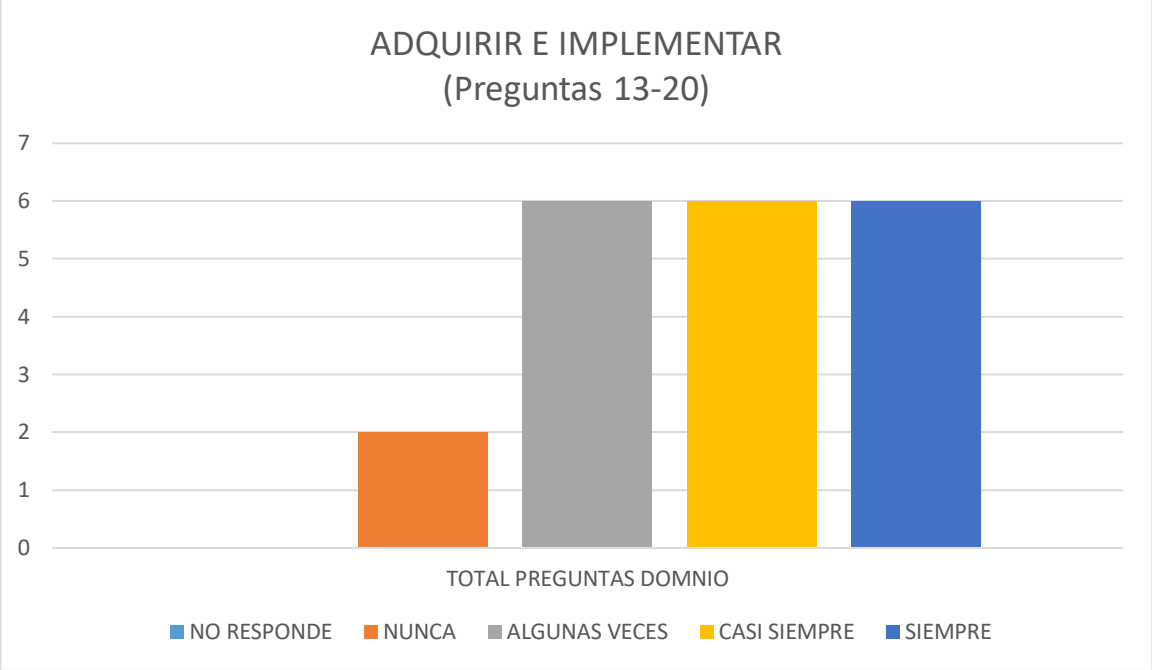


Fuente aplicada a PYMES concepción, 2016

Este grafico muestra el total de las respuestas del dominio de planear y organizar, en el cual observamos que este dominio en gran parte es logrado por las empresas porque se encuentran que los objetivos de la administración y la dirección de todos los recursos de TI están alineados con la estrategia de negocio.

Con esto la empresa genera o por lo menos sabe que debe tener una confianza en sus sistemas de información para lograr que su información sea confiable y segura, facilitando la toma de información.

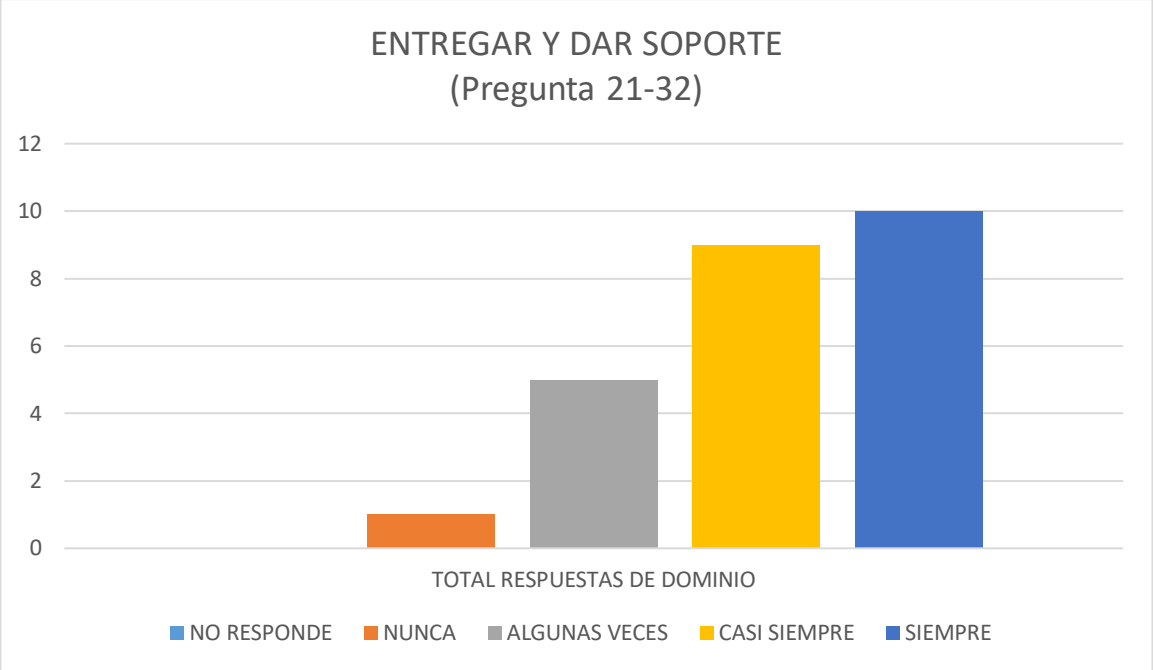
ADQUIRIR E IMPLEMNTAR



Fuente aplicada a PYMES concepción, 2016

Este grafico muestra el total de las preguntas de adquirir e implementar, en el cual se ve que las empresas están conscientes de que se deben aplicar soluciones TI y mostrarlo a lo largo de la organización para generar seguridad del uso de TI y que a la vez cuando sea requerido se puedan hacer cambios necesarios previa evaluación, autorización y posteriormente implementación.

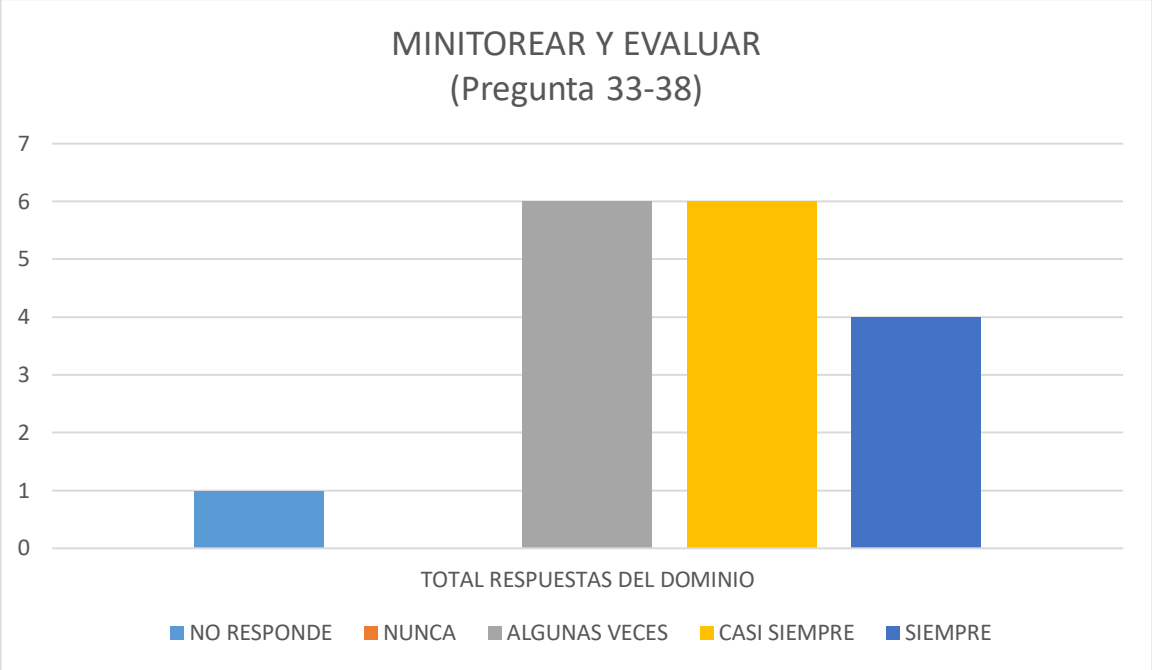
ENTREGAR Y DAR SOPORTE



Fuente aplicada a PYMES concepción, 2016

Este grafico muestra el total de respuesta del dominio entregar y dar soporte, en el cual se ve que las empresas saben que es importante después de haber implementado las soluciones del dominio anterior es imprescindible contar con respaldos y procesos que se revisen periódicamente.

MONITOREAR Y EVALUAR



Fuente aplicada a PYMES concepción, 2016

Este grafico muestra las respuestas totales del dominio monitorear y evaluar, en el cual se muestra que la preocupación de las empresas de cumplir con el control interno, el cumplimiento de las regulaciones y el desempeño del gobierno TI no es constante y predomina la poca preocupación de la gerencia.

CONCLUSION

Este trabajo tuvo como principal objetivo crear un manual de implementación de seguridad TI para Pymes, que ayudara a impedir que la información vulnerable sea robada o utilizada de mala forma.

Con los objetivos propuestos en esta investigación y posterior revisión de la información necesaria que permite realizar este estudio, se realiza una encuesta para saber el estado de las PYMES pero no influye en la creación del manual, solo se utiliza para saber que conocimientos tienes de la seguridad de información TI que se encuentra dentro de su organización.

Obteniendo como resultado un manual que primero identifica la información que se busca resguardar, luego de comprendido el significado de lo que se busca proteger, el siguiente paso es entregar las amenazas y vulnerabilidades existentes para posteriormente entregar los controles que servirán para implementar la protección en contra de las amenazas expuestas, seguido de esto se entregan formas para que la gerencia evalué si los controles se están llevando a cabo de buena forma y si están funcionando, como paso final se entrega un plan de continuidad que es opcional implementarlo por la gerencia ya que solo son medidas básicas que no remplazan un plan de continuidad del negocio que es llevado a cabo en mucho tiempo y con una inversión de recursos mayor.

Todos los controles entregados en esta investigación son necesarios para combatir posibles intrusos ya sea de personas ajenas o que pertenecen a la empresa siendo necesario la preocupación de los dueños o gerencia para concretar cualquier acción en pos de una seguridad de información que proteja a su activo más importante como lo es la información, el cual por su naturaleza tan amplia se vuelve difícil de controlar.

Se puede concluir que fue un trabajo interesante que acerco la seguridad de información TI siendo respaldado por CISA capítulo 5 que habla de la protección de los activos de información y también apoyado en las buenas practicas que es COBIT 4.1, fue de gran ayuda para conocer mejor el tema y saber que las PYMES necesitan tener una conciencia de seguridad de información que sea mejorada en el tiempo y vaya de la mano con el crecimiento de su negocio, permitiendo un amplio conocimiento de la empresa enfocándose y preocupándose de todas las áreas que constituyen el negocio.

Fue un gran aprendizaje esta investigación que me permitió interiorizar en un tema que solo conocía superficialmente, lo cual me ayudo a tener una mayor visión del mundo se seguridad de información y de las empresas que en muchas ocasiones no consideran como un tema importante porque nunca se han visto afectadas pero luego de sufrir algún ataque se preocupan de implementar medidas, sin embargo en la actualidad no se puede dejar puntos vulnerables pensando que nada va a ocurrir, siempre se debe estar atento frente a cualquier señal entregada por los sistemas.

El trabajo realizado requirió mucho esfuerzo, dedicación y trabajo constante, pero fue gratificante cuando comprendí la importancia de lo que estaba realizando y que día a día se va volviendo un tema que es tratado en muchas empresas entendiendo su importancia para el resguardo de su información y la implementación de un manual que guie con las medidas básicas de seguridad de información TI.

BIBLIOGRAFIA

- IT Gobernante Institute COBIT 4.0, 2008

- Manual preparación examen CISA 2008, ISACA. (CAPITULO 5).

- Evaluación de la seguridad de los sistemas de información apoyados por TI en la pequeña y mediana empresa utilizando estándares y buenas prácticas.
  Susana A. Espinoza Venegas, Carolina A. Vega Melo (2012).

- ISO 27001, 2013

- ISO 17799,2005

LINKGRAFIA

- Sistemas de información (en línea)
  http://biblioteca.itson.mx/oa/dip_ago/introduccion_sistemas/index.htm
  Consulta 20 de octubre de 2015
- Concepto de seguridad informática
  http://definicion.de/seguridad-informatica/
  Consulta 15 de diciembre de 2015
- Como crear un manual de procedimientos
  http://www.ingenieria.unam.mx/~guiaindustrial/diseno/info/6/1.htm
  Consulta 20 de febrero de 2016
- Seguridad de información
  http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1
  Consulta 25 de febrero de 2016

ANEXO

UNIVERSIDAD DEL BÍO-BÍO
FACULTAD DE CIENCIAS EMPRESARIALES

ENCUESTA DE BUENAS PRÁCTICAS PARA SEGURIDAD DE INFORMACIÓN TI

I. DATOS GENERALES

Nombre de la empresa:

…….

1. Actividad económica

   Indique: ……..

2. Existe una unidad especializada en TI dentro de la organización

   SI ……
   NO ……

3. De quien depende el encargado de la unidad de TI

A. Gerente general
B. Gerente de Administración y Finanzas
C. Jefe de informática
D. Otro ¿Quién? …….

II. PLANEAR Y ORGANIZAR

Este dominio tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio.

Marque con una cruz la alternativa correcta:

AFIRMACION	No responde	Nunca	Algunas veces	Casi siempre	Siempre
1. Las estrategias del negocio y de TI están alineadas.					
2. Se evalúa el desempeño de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.					
3. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura.					
4. Analizar las tecnologías existentes y emergentes para planear que dirección tecnológica es la apropiada para materializar la estrategia de TI y la arquitectura de sistemas del negocio.					
5. La dirección de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidad y supervisión.					
6. Existe un presupuesto definido para la inversión en TI.					

7. La empresa identifica y controla los costos/beneficios de la inversión realizada en TI.					
8. La gerencia (o dueños) asumen la responsabilidad de comunicar las políticas de control interno a la unidad de TI.					
9. Se verifica de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia.					
10. Existen actividades que permiten revisar la calidad de los proyectos y operaciones TI.					
11. Existe un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.					
12. La gerencia ha establecido y mantiene un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la Administración de proyectos.					

III. ADQUIRIR E IMPLEMENTAR

Este dominio se refiere a como las soluciones de TI son identificadas, desarrolladas o adquiridas, así como la implementación e integración para satisfacer los procesos del negocio.

AFIRMACION	No responde	Nunca	Algunas veces	Casi siempre	Siempre
13. Existen iniciativas que permiten identificar nuevas necesidades de aplicaciones tecnológicas, para facilitar el logro de los objetivos del negocio.					
14. Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio.					
15. La organización cuenta con procesos para adquirir, implementar y actualizar la infraestructura tecnológica.					
16. La dirección TI frente a nuevos sistemas genera documentación y manuales para usuarios y para TI.					
17. Los procesos de seguridad del uso de las TI están integrados a lo					

largo de toda la organización.					
18. Existe preocupación de que las adquisiciones satisfacen los requerimientos del negocio.					
19. Los cambios de los sistemas de TI, previamente a su implementación se:					
19.1.Registran					
19.2.Evalúan					
19.3.Autorizan					

20. Existe un proceso definido de adquisición de:

20.1 Hardware SI…… NO……

20.2 Software SI…… NO……

20.3 Servicios TI SI….. NO……

IV. ENTREGAR Y DAR SOPORTE

Este dominio cubre la entrega en sí de los servicios requeridos.

AFIRMACION	No responde	Nunca	Algunas veces	Casi siempre	Siempre
21. Con todo documentado es posible una adecuada comunicación entre la gerencia TI y los usuarios de los servicios requeridos.					
22. Establecer procesos de monitoreo para el cumplimiento de servicios de los proveedores.					

23. En caso de interrupción de un servicio TI, no hay problemas porque se dispone de un plan de contingencia.					
24. La administración de seguridad es suficiente para mantener la integridad de la información y de proteger los activos TI.					
25. Es equitativa la relación entre la necesidad y el costo TI asignado para un sistema acorde a lo requerido.					
26. Los procesos de seguridad (respaldo) se realizan periódica y regularmente en la empresa.					
27. El uso efectivo y eficiente de las soluciones y aplicaciones tecnológicas por parte de los usuarios, se logra mediante una capacitación adecuada.					
28. La dirección encargada de TI responde de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI.					
29. Se dispone de un procedimiento para identificar problemas, sus causas y soluciones que estén asociadas a las TI.					
30. La administración efectiva de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.					

31. Existen las instalaciones adecuadas para el equipo y el personal.					
32. Los servicios de TI entregados por terceros se revisan periódicamente y se retroalimenta sobre su desempeño para que mejore la calidad del servicio entregado.					

V. MONITOREAR Y EVALUAR

Este dominio indica que todos los procesos de TI deben evaluarse de forma regular en el tiempo, en cuanto a su calidad y cumplimiento de los requerimientos de control.

AFIRMACION	No responde	Nunca	Algunas veces	Casi siempre	Siempre
33. Una efectiva administración del desempeño de TI requiere un proceso de monitoreo.					
34. Se controla si las TI satisfacen lis requerimientos del negocio.					
35. Se realiza un control interno en la unidad de TI, para realizar mejoras o correcciones en los sistemas.					
36. Una supervisión efectiva garantiza que se cumplan las leyes y regulaciones vigentes.					
37. Las soluciones informáticas están alineadas con la					

	estrategia de negocio de la empresa.					
38.	La infraestructura de TI está organizada de modo tal que permite responder a una administración efectiva y eficiente del negocio.					

ANEXO 2

EXTRAIDO DE DOCUMENTO ORIGINAL

CAPITULO 5 CISA