UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMATICA

TESIS DE GRADO

"IMPLEMENTACIÓN DE LA METODOLOGÍA ITIL V3 DENTRO LA SEGURIDAD EN ENTIDADES PUBLICAS O PRIVADAS"

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMATICA
MENCION: INGENIERIA DE SISTEMAS INFORMATICOS

POSTULANTE: Alexander Omar Ustares Ocampo
TUTOR: Lic. German Huanca
REVISOR: M.Sc. Carlos Mullisaca

LA PAZ – BOLIVIA
2010

DEDICATORIA

A Dios por haberme fortalecido y cuidado en los momentos más difíciles.

A mi mamita Rosa, que Dios me la cuide y proteja, porque ella siempre ha creído y confiado en mí. Porque fuiste la mejor madre y padre a la vez, le agradezco a Dios por haberme puesto en el mundo a tu cuidado, este trabajo es la muestra de lo que ha hecho tu esfuerzo, tus cuidados y tu fe en mí. Gracias Mamita tú fuiste y eres siempre mi luz en la oscuridad

AGRADECIMIENTOS

Agradezco a Dios por haber guiado mis pasos, por haber puesto en mi camino a todos aquellos que fueron parte de este trabajo.

A mi mamita Modesta, a mi querido tío Beno, a mis hermanos Gustavo, Marcelo, Zulma, Ariadne, Armando y Flavia (Cuca) por su apoyo y colaboración.

A los docentes de la Carrera que fueron parte de mi formación en estos años de estudio,

A mis grandes amigos, Mayoly, Carola, Cesi, Rene, Joso, Chicho Pablo, Michael, Cesar, quienes me brindaron todo el apoyo para poder seguir adelante y concluir este trabajo. A mi docente tutor de Taller de Licenciatura II, Lic. Germán Huanca por su guía y amistad en el transcurso de la elaboración de esta Tesis. A mi docente revisor M.Sc. Carlos Mullisaca, por su amistad, comprensión y colaboración durante la elaboración y conclusión del presente trabajo. A todos mis amigos y compañeros de la carrera de Informática.

Agradezco a todo el personal administrativo y de biblioteca por su colaboración y su tiempo ya que fueron parte esencial de este trabajo.

RESUMEN

La finalidad de este proyecto es la creación de un nuevo estándar para aplicar una protección dentro de una entidad u organización para obtener beneficios. Todo esto basado en la situación actual y problemática de nuestro país. Es por eso que realizó una investigación de la metodología ITIL V3 y de normas ISO para iniciar la propuesta, con el fin de ayudar a las Entidades por medio del análisis llegando a la conclusión que el problema se presenta.

Se evalúo la forma de proteger la información en las entidades dando como resultado varios huecos que afectan el traslado seguro de la información, además se encontró diversas técnicas para recuperar la información y también para protegerlas durante el análisis de estas. En las técnicas de protección de los datos se encontró una gran variedad de implementaciones que engloban parte de lo sugerido en este estándar.

Conscientes de esta situación se creó un modelo de estándar estableciendo una protección a los datos de manera integral llevando así a la propuesta que se presenta para ser una guía que protege el activo más importante de una empresa el cual son los datos y siendo integral ya que prevé que hacer en caso de que estas medidas preventivas ocurran dando lugar a una mayor minimización de la perdida de los datos.

El modelo está dividido en varios puntos, los cuales van desde la administración de las TI hasta la responsabilidad del usuario, haciendo énfasis en las actividades de la dirección informática, el cual no son respectivamente en materia de técnicas o herramientas para hacer una protección efectiva, sino que están enfocadas en la cultura informática que tiene el empleado.

PALABRAS CLAVES: *Seguridad de la Información, Gestión de Servicio, Itil V3., Itil V2, Cobit, ISO/IEC 27000, ISO/IEC 20000,Gestion de Servicios TI, TIC, Seguridad Perimetral, Entidades Públicas, Entidades Privadas, CMD, SLA, Métodos de recuperación de datos, Firewall, Corrupción en la red, Tecnologías de protección.*

ABSTRACT

The purpose of this project is the creation of a new standard to apply a protection within an entity or organization to obtain benefits. Everything this based in the present-day and problematical situation of our country. That's why ITIL V3 accomplished an investigation of the methodology and of standards ISO to initiate the proposal, with the aim of helping the Entities by means of analysis coming to the conclusion that the problem shows up.

Himself I evaluate the way of protecting the information at the entities giving as a result several holes that affect the safe informational transfer, besides found various techniques to recover the information and also to preserve them from during analysis these. One found a great variety of implementations that encompass part of what suggested in this standard in the techniques of protection of the data.

Conscious he created of this situation a model of standard establishing a protection to the data of comprehensive way taking the proposal that way for himself that it is gotten there to be a guide that preserves the more important assets from a company data are which and being comprehensive since you foresee making in the event these preventive measures happen causing a bigger minimization of the prostitute of the data.

The model is divided into several points, which go from the administration of them YOU to the user's responsibility, stressing the activities of the information-technology address, they are not which respectively on the subject of techniques or tools to do an effective protection, rather they are focused on the information-technology culture that the employee has.

KEYWORDS: *Informational certainty, Gestión on duty, Itil V3, Itil V2, Cobit, ISO/IEC 27000, ISO/IEC 20000, Question of Services TI, TIC, Seguridad Perimetral, Public Entities, Private Entities, CMD, SLA, Methods of data retrieval, Firewall, Corruptions in the net, protective Technologies.*

INDICE DE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO 1. MARCO REFERENCIAL

En este capítulo se presenta a manera de presentación los antecedentes del trabajo de implementación para la seguridad de la información, la definición del problema, sus objetivos, la hipótesis que buscamos demostrar y por ultimo sus alcances y aportes para el desarrollo del trabajo.

1.1. PRESENTACION

Los Sistemas de Información (SI) y las Tecnologías de Información (TI) han cambiado la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, ya que automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implantación logra ventajas competitivas.

Las Tecnologías de la Información han sido conceptualizadas como la integración y convergencia de la computación, las telecomunicaciones y la técnica para el procesamiento de datos, donde sus principales componentes son: la información, el equipamiento, el factor humano, la infraestructura, el software y los mecanismos de intercambio de información, los elementos de política y regulaciones, además de los recursos financieros. [www, 1].

Los negocios tienden a tener una mayor dependencia de las Tecnologías de la Información. Los departamentos de Sistemas de Información y las actividades en ellos desarrolladas han sido tradicionalmente vistos como un área de soporte al negocio, descuidando incluso muchas veces el uso de criterios racionales para medir su rentabilidad, eficacia y la calidad del servicio ofrecidos a toda la organización. [Donoso, 2006].

Information Technology Infraestructure Library (ITIL), es una metodología que se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos que cubren las actividades más importantes de las organizaciones en sus Sistemas de Información y Tecnologías de Información. Esta metodología fue desarrollada a petición del Gobierno del Reino Unido a finales de los 80 y recoge las mejores prácticas en la gestión de los Sistemas de Información. Desde entonces se ha ido extendiendo su uso en toda la empresa privada, tanto multinacional como PYME, llegando a ser considerado un estándar de facto para la gestión de esta área de la empresa. [Donoso, 2006].

En un entorno donde los periodos de disponibilidad de los servicios son cada vez más amplios, donde las exigencias del cliente son cada vez más elevadas, donde los cambios en los negocios son cada vez más rápidos, es muy importante que los Sistemas de Información estén adecuadamente organizados y alineados con la estrategia del negocio. ITIL propone la gestión de estos Sistemas mediante 10 procesos, con un claro enfoque a la Gestión del Servicio. Igualmente ITIL, ofrece toda una serie de definiciones de conceptos típicos de los Sistemas de Información para garantizar que todos sus conocedores hablen de lo mismo, reduciendo así los tiempos y riesgos por malas interpretaciones. [Ramírez, 2006].

A medida que las redes pasan a ser un elemento integral de las corporaciones, las tecnologías de seguridad de red se desarrollan para proteger datos y preservar la privacidad. El test de seguridad en una red permite identificar vulnerabilidades y asegurar los requisitos de seguridad de cualquier empresa. El análisis de la seguridad permite reconocer información maliciosa, tráfico no autorizado, vulnerabilidades de dispositivos o de la red, patrones de intrusión, y extraer conclusiones de la información recopilada en el test. Entonces, ¿dónde está el problema? Uno de los grandes logros de la versión 3 es haber elevado las TI a los altares de la empresa, situándolas en el nivel estratégico.

Como consecuencia de ello ITIL ha dejado de ser un acrónimo de uso corriente exclusivamente entre los responsables de sistemas y/o seguridad para pasar a formar parte del léxico habitual de la dirección. [Marina, 2009].

En este sentido lo que se plantea en este trabajo es implementar políticas de gestión de cambios adecuadas que evite o al menos controle los cambios no autorizados. En otras palabras se contempla el diseño de servicio apropiados e innovadores, incluido su arquitectura, procesos, políticas y documentación, dentro el departamento de sistemas en entidades públicas, para alcanzar los requerimientos actuales y futuros acordados.

Uno de los pilares centrales de ITIL, la Base de Datos de la Gestión de Configuraciones (CMDB: Configuration Management Data base) juega un papel primordial en este sentido habida cuenta que permite seguir el rastro de todos los componentes TI y mantener la relación entre ellos. CMDB se convierte así en una pieza clave para poder gestionar el servicio dentro de los parámetros de seguridad y calidad fijados.

ITIL v3 va un poco más lejos al incorporar los conceptos de Sistema de Gestión de la Configuración (CMS: Configuration Management System) – conjunto de repositorios que soportan la gestión de la configuración- y de Sistema de Gestión del Conocimiento (SKMS: Servicie Knowledge Managament System). [Marina, 2009].

1.2. ANTECEDENTES

En la actualidad no existen proyectos y/o tesis de grado en la carrera de informática en la que intervenga la metodología ITIL, ya que es una metodología desconocida y que recientemente se está incorporando en nuestro medio dentro las organizaciones para organizar y fundar las mejores prácticas de la gestión de servicio TI.

Los negocios ya no son como hace años, las organizaciones han cambiado y se necesita destacar en la calidad de los servicios TI. En el mundo de las TIC ahora se

está empezando a implantar las mejores prácticas ITIL para optimizar el uso de los recursos informáticos, alineando los objetivos específicos de seguridad con los objetivos generales del negocio. Y el primer paso es que la dirección asuma su responsabilidad, que puede llegar incluso al ámbito legal, en la protección de los activos de su empresa.

Es importante reconocer que las I.T. (Tecnologías De Información) no pueden estar implementadas en una organización ya sea pública o privada, sin que ella esté articulada al diseño estratégico de la empresa; para ello se debe contar con un modelo de diseño estratégico de negocios. [www, 2].

Dentro del modelo de buenas prácticas ITIL, y centrándose en seguridad TIC, la Gestión de la Seguridad es de vital importancia, se contempla en forma de proceso y también participa en la entrega del Servicio. ITIL no solo aporta beneficios a la gestión del servicio TI, también ayuda y facilita a la Gestión de la Seguridad.

Ésta, se relacionada con prácticamente todos los otros procesos TI y necesita para su éxito, la colaboración de toda la organización. Los procesos ITIL "Gestión de la Continuidad del Servicio TI" y "Gestión de la disponibilidad", protegen el grado de disponibilidad de los activos de la información. Los demás procesos, facilitan la ejecución de otras actividades de la Gestión de la Seguridad tales como el tratamiento de incidencias de seguridad, clasificación, implantación de controles a través de la gestión de cambios, gestión de la configuración y gestión de la entrega. [www, 3].

Es necesario realizar también, un control del proceso para asegurar que la Gestión de la Seguridad cumpla con sus objetivos. Si se realiza una correcta Gestión de la Seguridad:

- Se reducen el número de incidencias relacionadas con la seguridad.

- Los accesos a la información de la empresa, serán eficaces y solo por el personal autorizado en base a los parámetros de confidencialidad, integridad y disponibilidad.
- Se identificaran vulnerabilidades antes de que estas se manifiesten y provoquen un problema en la calidad del servicio ofrecido.

Por lo tanto, si se toman medidas a tiempo, minimizaremos la probabilidad de que afecten directamente a nuestro negocio y que nos causen un daño importante.

Hay que tener en cuenta que ITIL es aplicable de manera moldeable a cualquier organización. Esto no es rígido, ya que son una serie de buenas prácticas. Hay que tener bien definido en que terreno nos encontramos actualmente, procesos, estructura organizacional, etc. con tal de definir la mejor estrategia de negocio. La versión 3 de ITIL interactúa mayor mente con la gestión de procesos, por lo que hay que tener en cuenta un control total sobre nuestras acciones, para no llegar a un punto donde nuestra productividad aumente pero con una disminución total en nuestra calidad. [www, 4].

1.3. DEFINICIÓN DEL PROBLEMA

Actualmente nos encontramos con la enorme paradoja de que los mayores recursos humanos y económicos se han venido dedicando a combatir la amenaza externa, descuidando por el contrario la amenaza interna, cuando es esta última la que más quebraderos de cabeza provoca en materia de seguridad. ¿Cuántas veces lo que era aparentemente un sencillo cambio en la configuración de la infraestructura interna o la rutinaria creación de un nuevo perfil de usuario han provocado fallos dejando al descubierto la vulnerabilidad de nuestra política de seguridad? Hemos invertido sobradamente en seguridad perimetral (cortafuegos, sistemas de monitorización y detección de intrusión, control de acceso, etc.) que nos protege del exterior pero no hemos sido igual de cautos (o previsores) a la hora de vigilar y controlar los cambios en la infraestructura TI. La realidad es que nadie puede entrar sin nuestro permiso y

conocimiento pero casi cualquiera puede cambiar la configuración al no tenerla definida.

Las metodologías y normas desarrolladas para combatir las amenazas tanto internas como externas dentro de una entidad u organización llegan a ser muy complejas para su incorporación e implementación dentro de estas, y mucho más para organizaciones pequeñas puesto que les es difícil adecuar estas metodologías a sus estructuras.

Los procesos con la que cuenta la metodología ITIL V.3 pueden ser adecuados a cada situación y cada organización o entidad por parte de los profesionales o personal encargado de la seguridad de los sistemas informáticos, brindando soporte en el diseño estratégico, articulado a los procesos de negocios y los procesos corporativos, en el que debe integrarse y articularse lo gerencial, lo estructural, lo individual y lo institucional; siempre ellos soportados en bases de datos de sistemas de información.

A raíz de los estudios realizados sobre el funcionamiento interno actual dentro de entidades públicas, se han detectado diversos problemas:

- El sistema de infraestructura de tecnologías de la información y comunicación sigue un patrón de comportamiento reactivo ante los problemas que va surgiendo.
- Los mecanismos de funcionamiento de no están bien organizados y esto provoca que los mismos problemas o incidencias se repitan, no haya un tiempo estándar establecido para resolver los mencionados problemas, etc.
- Las diferentes personas que trabajan con los sistemas TIC no tienen bien delimitadas sus funciones, y esto provoca problemas a la hora de resolver problemas en el sistema y a la hora de atender las incidencias que los clientes nos hagan llegar. De esta forma, cualquier circunstancia ante la cual haya que actuar difícilmente será cubierta por la persona más indicada para ello.

- Al no ser capaces de detectar de forma eficiente los problemas en nuestro sistema, ni tampoco de registrarlos de forma ordenada y consciente, no se tienen bases para medir los niveles de calidad que nuestros proveedores nos dan, y por lo tanto de poder reclamar justificadamente el nivel de calidad de servicio contratado, defendernos de posibles engaños, etc.

- No es capaz de establecer un nivel de calidad de servicio y cumplirlo de forma garantizada.

- Al haber tanta heterogeneidad de recursos (plataformas y sistemas operativos diferentes, móviles y PDAs con conexión a Internet, variedad de aplicaciones dedicadas y otras genéricas, telefonía sobre IP prevista para un futuro, acceso cableado e inalámbrico a la red, oficinas distribuidas, etc.), se hace muy compleja la gestión del sistema por el hecho de no disponer de un sistema de gestión totalmente integrado.

Ante la existencia de estos problemas se construye la pregunta de investigación.

¿La incorporación de la metodología ITIL V.3 dentro las normas diseñadas para el manejo de los activos de las unidades de sistemas, solucionara el problema de amenazas externas e internas?

1.4. JUSTIFICACION

1.4.1. Justificación Teórica

Al existir varias Metodologías referidas u orientadas a la seguridad Informática hace dificultosa la elección y la aplicación de alguna de estas en una organización que hace uso de software para realizar el control de tráfico y el comportamiento de la información al interior de estas y en sus diversas áreas donde se toma en cuenta las

aplicaciones que brindan seguridad en sus procesos. Este hecho dificulta la comprensión, aplicación e implementación por parte de los profesionales y los miembros de las organizaciones que se encargan en realizar este tipo de control. Este trabajo de investigación sobre la implementación de los procesos Metodológicos de ITIL V.3 para la seguridad informática, aporta con información para brindar una mayor comprensión sobre el manejo de servicios a través del ciclo de vida, por medio de estrategia, transición, operación y mejoramiento continuo.

1.4.2. Justificación Social

Al implementar los procesos de la metodología ITIL V.3 dentro la estructura de las entidades públicas, se podrá diseminar las mejores prácticas en la gestión de seguridad de la Información de forma sistemática. Por otra parte este trabajo de investigación beneficia a estudiantes, profesionales y personas que quieran tener un mejor acercamiento de Gestión de Negocio y de Gestión de Servicio TI, su razón toma forma de funciones y procesos que busca mejorar el nivel o calidad de servicio comenzando por la planificación pasando por su utilización y seguimiento.

1.4.3. Justificación Económica

El principio de esta metodología está especialmente desarrollada para reducir los costos de provisión, soporte de los servicios de TI, en el momento de combatir amenazas tanto internas como externas y ver el impacto sobre las políticas de seguridad existentes, es decir al dar valor añadido a la gestión de seguridad de la información podremos controlar y evaluar mejor nuestros recursos tecnológicos y económicos.

1.5. OBJETIVOS

1.5.1. Objetivo General

Incorporar dentro la documentación y normas diseñadas específicamente para las unidades de sistemas los procesos basados en la metodología ITIL V.3 para la

gestión de seguridad y servicios TIC que asista y que permita identificar amenazas y riesgos existentes en las unidades de sistemas de las en entidades u organizaciones.

1.5.2. Objetivos Específicos

- Realizar el diseño de la estrategia servicio dentro las organizaciones.
- Aplicar procedimientos que tiendan a evaluar componentes de apreciación del riesgo, ambiente de control, actividades de control y supervisión.
- Analizar y comprobar el funcionamiento de control interno para establecer lineamientos de trabajo en las unidades de sistemas.
- Hacer énfasis en la aplicación de la metodología ITIL V.3 para el desarrollo de las actividades, que permitan evaluar y minimizar los riesgos futuros.

1.6. HIPOTESIS

Es posible ajustar la Metodológica ITIL V.3 con la finalidad de obtener tareas y procesos encerradas en una norma que colabore al área de sistemas, mejorando la seguridad de la información dentro de las unidades informáticas tomando en cuenta el impacto que estos producen a la organización.

1.6.1. Identificación de Variables

Variable independiente: La metodológica ITIL V.3 a ser implementada en los procesos de seguridad de la información dentro las unidades informáticas de las entidades.

Variable dependiente: Todos los componentes TI. en explotación (en funcionamiento).

1.7. ALCANCES Y APORTES

1.7.1. Alcance

El presente trabajo de investigación propone el diseño de estrategias y de gestión de servicios dentro la documentación de procesos de las unidades de sistemas, las cual está basada en la metodología ITIL V.3 dentro de las entidades, aplicando normas para reducir la vulnerabilidad de estas.

La información de esta investigación puede ser de utilidad para las unidades de sistemas de las organizaciones y de personas interesadas en la aplicación de normas de seguridad y los procesos que intervienen esta.

1.7.2. Aportes

Los aportes presentados por este trabajo están principalmente orientados a brindar solución a la falta de normas en el manejo de la información donde intervienen las TIC. Por lo que más de presentar otra norma, lo que se quiere que sea es una herramienta en el manejo de la información.

De esta manera este trabajo proporciona aportes al área de seguridad de la información y manejo de las TIC.

1.8. METODOLOGIA

1.8.1. Métodos y etapas de la Investigación Científica

El método de investigación científica identifica varios tipos de desarrollo que se adecuan a los propósitos que persigue una investigación. En este trabajo de investigación se realizara sobre los lineamientos de la investigación científica experimental, que basa su razón en el uso de una variable experimental no comprobada, en condiciones rigurosamente controladas, con el fin de describir de qué modo o la causa se produce una situación o acontecimiento particular. Las etapas que se establecen para este trabajo son:

- Elección del tema de Investigación
- Identificación y definición del problema
- Definición de hipótesis y variables
- Diseño de plan experimental
- Prueba de confiabilidad de datos
- Realización de experimento
- Tratamiento de datos

CAPÍTULO 2. MARCO TEÓRICO

En este capítulo se analiza el tema de la Seguridad de la Información, análisis de la metodología ITIL, su definición, objetivos, técnicas, y los pasos que se deben seguir en las tareas de Gestión de los Servicios TI y las normas con las que trabaja.

2.1. SEGURIDAD DE LA INFORMACIÓN.

La información es lo que se conoce como un activo. Un activo es un elemento que tiene valor para una organización.

La información, además, puede ser un activo tangible o intangible. Es decir, no solamente tenemos que pensar en información almacenada en los ordenadores o en un disco duro. La información también podemos encontrarla en formato papel, en una cinta magnética, en un CD o en una nota colocada encima de la pantalla de nuestro ordenador.

¿Por qué es valioso un activo para una organización? La respuesta está en la propia organización. Si nos fijamos en una organización cualquiera, vemos que la información que es importante para una organización es relevante para su actividad ya que en torno a ella se crean y desarrollan un conjunto de procesos y tareas. Sin la información, esos procesos y tareas no sirven de nada y no es posible llevarlos a cabo adecuadamente. [Inteco, 2008].

La información, además de las características comentadas, posee otras que determinan la forma en que la utilizamos, y por supuesto, la protegemos. La información proviene de diversas fuentes y se presenta en distintos soportes. Además, la información se transmite a través de distintos medios y tecnologías.

Asimismo, hay que ser conscientes de que la información tiene un ciclo de vida, es decir, durante el tiempo que la información es utilizada pasa por un conjunto de

fases: se crea, se difunde, se transmite, se copia, se modifica, se almacena y, a partir de un momento determinado, deja de ser útil o se convierte en información obsoleta, lo que supone su archivado o destrucción, con lo que llegamos al final de su ciclo de vida. [Inteco, 2008].

A partir de todo lo anterior, estamos en disposición de definir, de una forma comprensible, qué es la Seguridad de la Información.

La Seguridad de la Información es la protección de tres aspectos o facetas de la información, que son las siguientes:

- Confidencialidad: consiste en evitar que personas, programas o sistemas no autorizados puedan acceder a ella sin autorización.
- Integridad: es la característica de la información relativa a su fiabilidad. Su protección consiste en que la información no sea alterada o modificada sin autorización.
- Disponibilidad: este aspecto hace referencia a que la información esté accesible, es decir, disponible para su utilización cuando sea necesaria.

2.1.1. La Seguridad de la Información desde el punto de vista del negocio.

La Seguridad de la Información abarca múltiples aspectos de una organización, no se trata únicamente de cuestiones técnicas, sino también de aquellas relativas a cuestiones organizativas, de procedimiento, de políticas, de responsabilidad, etc.

Por otro lado, la Seguridad de la Información no es competencia exclusiva de los responsables de sistemas de una organización sino que todos los miembros de una organización tienen parte de responsabilidad en mantener un adecuado nivel de seguridad.

Vamos a conocer cuáles son los aspectos fundamentales de las organizaciones sobre los que la Seguridad de la Información nos puede ayudar a mejorar nuestra organización. Como vamos a ver, son básicamente tres:

- La responsabilidad y la productividad.
- La imagen y la competitividad.
- La capacidad para superar contingencias y la continuidad del negocio.

Estos tres grandes grupos engloban la mayoría de los aspectos relativos a cualquier organización en los cuales la Seguridad de la Información nos puede ser de gran ayuda a la hora de mejorarlos. [Inteco, 2008].

2.1.2. La Seguridad de la Información desde el Punto de Vista de las Amenazas.

Para comprender con más claridad el contenido del presente subtitulo avancemos algunos conceptos sobre los tipos de amenazas que existen y que vamos a ver a lo largo de este apartado.

- Subculturas. Hackers, phreakers, hacktivistas, etc. Son el origen de muchas amenazas TIC y es necesario conocer su existencia.
- Malware. Virus, troyanos, ad-ware, keyloggers, etc. Es la base de múltiples técnicas y amenazas. Algunos de ellos llevan con nosotros desde el nacimiento de los ordenadores hasta la actualidad.
- Ingeniería social. Spam, fraude bancario, robo de identidad, etc. Se ha convertido en una de las amenazas principales del uso de las tecnologías de la información e internet. Es la base para múltiples delitos e incidentes de seguridad.
- «El enemigo está dentro». Hasta hace poco se consideraba que la mayoría de las amenazas provenían del exterior de las organizaciones pero cada vez se producen más incidentes de seguridad cuyo origen es la propia organización.

Lamentablemente, las organizaciones criminales han pasado a sustituir a aquellos hackers por algo mucho más siniestro y peligroso. Hoy en día los grupos de

delincuencia organizada han encontrado en internet una nueva frontera para cometer delitos.

Las organizaciones y las empresas se han convertido en nuevos focos de incidentes de seguridad poniendo a sus propios empleados en el punto de mira. Se ha acuñado la expresión «el enemigo está dentro» para referirse a este fenómeno.

Estos cuatro grupos no son más que una de las múltiples formas en las que podemos agrupar las amenazas TIC que existen en la actualidad. [Inteco, 2008].

2.2. DIFERENCIA ENTRE DATO E INFORMACIÓN.

Los datos describen únicamente una parte de lo que pasa en la realidad y no proporcionan juicios de valor o interpretaciones, y por lo tanto no son orientativos para la acción. La toma de decisiones se basará en datos, pero estos nunca dirán lo que hacer. Los datos no dicen nada acerca de lo que es importante o no. A pesar de todo, los datos son significativos para las organizaciones, ya que son la base para la creación de información.

A diferencia de los datos, la información tiene significado (relevancia y propósito). No sólo puede formar potencialmente al que la recibe, sino que está organizada para algún propósito. Los datos se convierten en información cuando su creador les añade significado. Se transforman los datos en información cuando se les añade valor en varios sentidos. Hay varios métodos:

- Contextualizando: Se conoce el para qué propósito se generaron los datos.
- Categorizando: Se conocen las unidades de análisis de los componentes principales de los datos.
- Calculando: Los datos pueden haber sido analizados matemática o estadísticamente.
- Corrigiendo: Los errores se han eliminado de los datos.

- Condensando: Los datos se han podido resumir de forma más concisa.

2.3. PROTECCIÓN DE DATOS.

"Medidas de prevención del uso indebido e indiscriminado de los datos personales contenidos en bases de datos." [www, 7].

Esta definición, genera una idea general de lo que se define como protección de datos, pero no se usará esa definición, ya que está muy limitada a lo que son simplemente las bases de datos, por lo que resultaría excluyente de los archivos planos que utilizan los bancos e instituciones financieras para el procesamiento de datos.

Sin embargo, se utilizará esa definición como base para plantear lo siguiente:

La protección de datos se refiere a las medidas de prevención del uso indebido e indiscriminado de los datos, contenidos en sistemas informáticos.

Habrá de delimitar a los sistemas informáticos ya que esta investigación se enfoca al área informática.

En el intento por proteger los datos, se han creado normas y regulaciones para mejorar la protección de los datos y definir también que es lo que se debe de proteger.

Uno de los más grandes problemas fue solucionado por la Ley Orgánica de Protección a los Datos (LOPD) ya que entre sus regulaciones define qué tipo de dato es privado y cual de acceso público, de manera general.

2.4. RECUPERACIÓN DE DATOS.

Antes de hablar de recuperar datos, es necesario conocer por que debiera recuperarse un dato, esto es debido a que siempre que se generé información existirá por lo menos una entrada de carácter humano, por lo cual al tratarse de

personas, siempre ex iste un nivel de incertidumbre que varía conforme a la confianza, experiencia y valores de esta.

La recuperación de datos se da a partir de la perdida de estos. Esta pérdida se puede deber a diversas causas, y puede conllevar a diversos métodos para su recuperación la cual en la mayor parte de los casos.

Existen diversos factores que pueden ocasionar la necesidad de recuperar información tales como el borrado no intencionado de archivos por un error "de dedo", o "el descubrimiento de que el ordenador tenía un virus que mi antivirus no elimino", o detalles como este que a todos nos ha pasado.

La recuperación de datos es el conjunto de métodos y herramientas para recuperar los datos que contienen la información necesaria para realizar alguna tarea.

2.5. PERDIDA DE DATOS.

Algunas veces cuando se trabaja en extensos proyectos o escritos, como este, en donde se hacen participes más de una persona y se envían archivos mediante las diversas técnicas de comunicación existente, se expone al riesgo de perder información valiosa en la que se ha invertido tanto tiempo y esfuerzo, esto ya sea por algún virus de reciente manufactura, o se encontraba uno cansado y pego mal el documento con la sección A en la sección C y la B en la sección A haciendo un verdadero desorden en su trabajo. [Scambray, 2002].

Muchas veces al corregir estos errores, se ha "perdido" información debida a la falta de algún dato que no está, o se le olvido guardar el documento y su procesador de palabras, no auto guardó esos cambios.

Muchas veces y muchas personas se han encontrado con algún caso parecido, si es que no idéntico al mencionado anteriormente, a esto se le llama

simplemente la perdida de información, pero ¿realmente se pierde la información o se pierden datos?

La ausencia total o parcial de la representación simbólica, atributo o característica de una entidad en un sistema informático es lo que se definirá como perdida de datos.

2.6. CAUSAS DE PÉRDIDAS DE DATOS

Una causa es un factor causante de, en este caso es el factor causante de la perdida de los datos.

Las causas de la pérdida son variadas y probablemente muy distintas entre sí, ya que hay demasiadas maneras de dañar o extraviar datos, entre ellas se engloban las más comunes:

- Desastres Naturales
- La intrusión de algún Hacker o virus
- El error humano
- Falla en el hardware
- Falla en el software

Que son los más comunes y engloban la mayor parte de las causas de pérdida de información. [Scambray, 2002].

2.6.1. Desastres Naturales

La naturaleza se encuentra en un proceso permanente de movimiento y transformación, que se manifiesta de diferentes maneras, a través de fenómenos de cierta regularidad como la lluvia, los temblores, erupciones volcánicas y otros eventos que llegan a ocasionar daños tales como las inundaciones, deslizamientos de tierra, incendios.

En esta categoría de desastres naturales están todas aquellas causas que están fuera de nuestra capacidad para evitarlos, tales como el incendio de la oficina donde está el servidor, o los movimientos telúricos de la tierra, los tsunamis, inundaciones y las fallas eléctricas.

Esta última no es un desastre natural, pero está fuera de nuestra capacidad para evitar la pérdida de datos. [Scambray, 2002].

2.6.2. Errores Humanos

Esta categoría esta creada por todos las posibles causas debidas a la actividad humana, que para nuestra investigación resulta la más común, ya que por la condición humana se tiende a cometer pequeños incidentes que causan la perdida de datos, como por ejemplo el olvidar salvar el documento antes de dejar el equipo o guardar este archivo en el CD regrabable que prestaste antes de entregar a revisión.

También se debería englobar toda aquella actividad que intencionadamente cause la perdida de datos, mas sin embargo por tratarse de algo intencional se ha separado para tratar estos problemas de forma separada y sea más sencillo el metodizarlos. [Scambray, 2002].

2.6.3. Hackers

En esta categoría se encuentran todas aquellas actividades en la que interviene un tercero utilizando diversas técnicas para el robo de información y para causar un daño en el sistema informático.

Entre estos agentes están los “hackers”, programas de auto propagación tales como virus, gusanos, caballos de Troya y todo aquel software que perjudique a los equipos de cómputo.

2.6.4. Falla de Hardware y Software.

La falla de Hardware y Software es otra de las categorías más comunes, si es que no una de las principales causas de la perdida de datos.

La falla de software no es más que la posible secuela de la recuperación del sistema después de un ataque informático (virus, etc.) y que ha dejado rastros de su ataque alterando el correcto funcionamiento del sistema. También está el cuelgue del sistema operativo o del mismo sistema, definiendo como cuelgue de sistema cuando la computadora aun responde y nuestro programa queda pasmado.

El cuelgue del sistema operativo es una falla aún más grave ya que conlleva a la detención de todo programa o sistema ejecutado en el equipo que sufrió dicho percance, haciendo en algunos casos más difíciles la detección de la perdida de datos y su recuperación.

Las fallas de Hardware son debidas a problemas físicos, principalmente se da en los medios de almacenamiento tales como memorias, discos duros, y medios de almacenamiento móvil.

2.7. ITIL V3.

ITIL puede ser definido como un conjunto de buenas prácticas destinadas a mejorar la gestión y provisión de servicios TI. Su objetivo último es mejorar la calidad de los servicios TI ofrecidos, evitar los problemas asociados a los mismos y en caso de que estos ocurran ofrecer un marco de actuación para que estos sean solucionados con el menor impacto y a la mayor brevedad posible.

Sus orígenes se remontan a la década de los 80 cuando el gobierno británico, preocupado por la calidad de los servicios TI de los que dependía la administración, solicito a una de sus agencias, la CCTA acrónimo de Central Computer and Telecommunications Agency, para que desarrollara un estándar para la provisión eficiente de servicios TI.

En la actualidad es la OGC (Office of Government Commerce) el organismo encargado de velar por este estándar y la responsable de la última versión de ITIL (v3) que data del año 2007. [Osiatis, 2010].

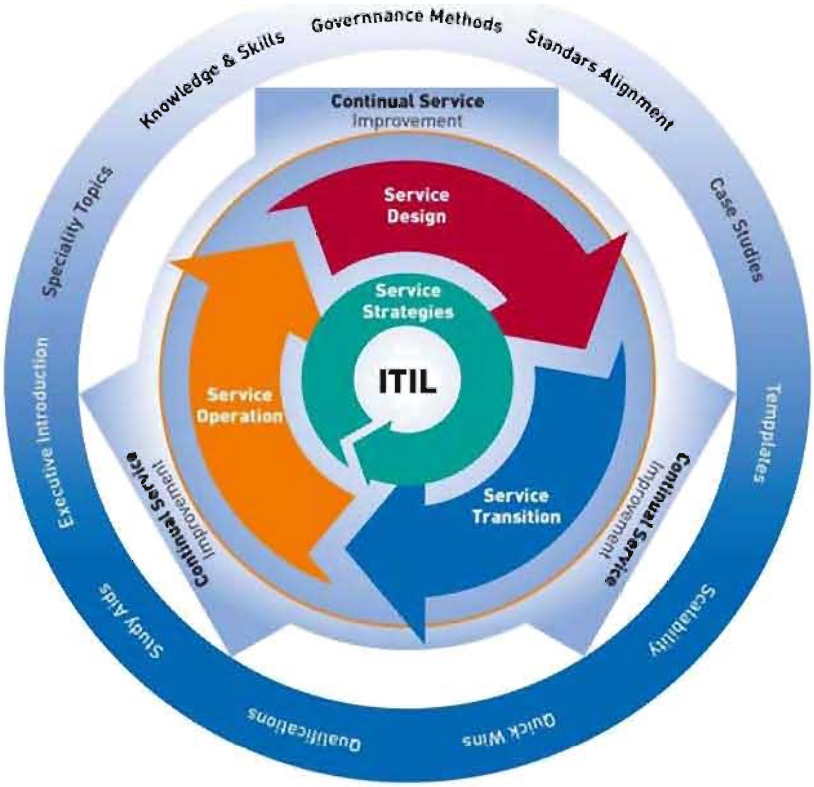


Figura1: La infraestructura ITIL.
Fuente: "Fundamentos de Itil V3." Ricardo Adrián Federico.

La OGC cuenta con la colaboración de varias organizaciones para el mantenimiento de ITIL:

- **itSMF:** El Information Technology Management Forum es una organización independiente y reconocida internacionalmente que tiene como principal objetivo impulsar la adopción de las mejores prácticas ITIL para la gestión de servicios TI.

- **APM Group:** Es una organización comercial encargada por la OGC de definir, publicar y gestionar las certificaciones ITIL así como de acreditar a los organismos examinadores.
- **Organismos examinadores:** En la actualidad existen varios organismos examinadores acreditados por APMG entre los que se encuentran EXIN, BCS/ISEB y LCS.

2.7.1. Gestión de Servicios TI.

La tecnología de la información es tan antigua como la historia del hombre y está a jugado gran papel en la misma. Pero, no ha sido hasta tiempos recientes que por medio de la automatización de su gestión que se ha convertido en una herramienta imprescindible y clave para organizaciones y empresas.

Hoy en día nadie duda de que la información es el recurso estratégico más importante que tiene cualquier organización y que para que la organización proporcione servicios TI de alta calidad es fundamental que se realice un análisis, producción y distribución de la información que maximicen dicha calidad.

La concienciación de que los servicios TI son cada vez más importantes para el negocio ha llevado a la introducción de la gestión de servicios TI. La gestión de servicios TI está dirigida a proporcionar datos para la toma de decisiones desde una perspectiva de procesos, y proporcionar una implementación profesional con responsabilidades bien definidas. Un prerrequisito de las organizaciones es una disposición incondicional tanto de dirección como del personal TI para centrarse en el cliente y en el servicio.

La gestión de servicios TI está compuesta por un conjunto de capacidades organizacionales especializadas para proporcionar valor a los clientes en forma de servicios. Tales capacidades incluyen funciones y procesos utilizados para gestionar los servicios a través de su ciclo de vida, con especializaciones en estrategia, diseño,

transición, operación y mejora continua. El acto de transformar recursos en servicios con valor es el centro de la gestión de servicios.

2.7.2. Objetivos Gestión de Servicio TI.

Los objetivos de una buena Gestión de Servicio TI han de ser:

- Alinear los servicios TI con las necesidades del negocio y sus clientes
- Mejorar la calidad de los servicios TI
- Reducir el coste en la provisión de servicios

2.7.3. El Ciclo de Vida de los Servicios TI.

ITIL v3 estructura la gestión de los servicios TI sobre el concepto de Ciclo de Vida de los Servicios.

Este enfoque tiene como objetivo ofrecer una visión global de la vida de un servicio desde su diseño hasta su eventual abandono sin por ello ignorar los detalles de todos los procesos y funciones involucrados en la eficiente prestación del mismo. [Business, 2009].

El Ciclo de Vida del Servicio consta de cinco fases que se corresponden con los nuevos libros de ITIL:

- Estrategia del Servicio: propone tratar la gestión de servicios no sólo como una capacidad sino como un activo estratégico.
- Diseño del Servicio: cubre los principios y métodos necesarios para transformar los objetivos estratégicos en portafolios de servicios y activos.
- Transición del Servicio: cubre el proceso de transición para la implementación de nuevos servicios o su mejora.
- Operación del Servicio: cubre las mejores prácticas para la gestión del día a día en la operación del servicio.

- Mejora Continua del Servicio: proporciona una guía para la creación y mantenimiento del valor ofrecido a los clientes a traces de un diseño, transición y operación del servicio optimizado.

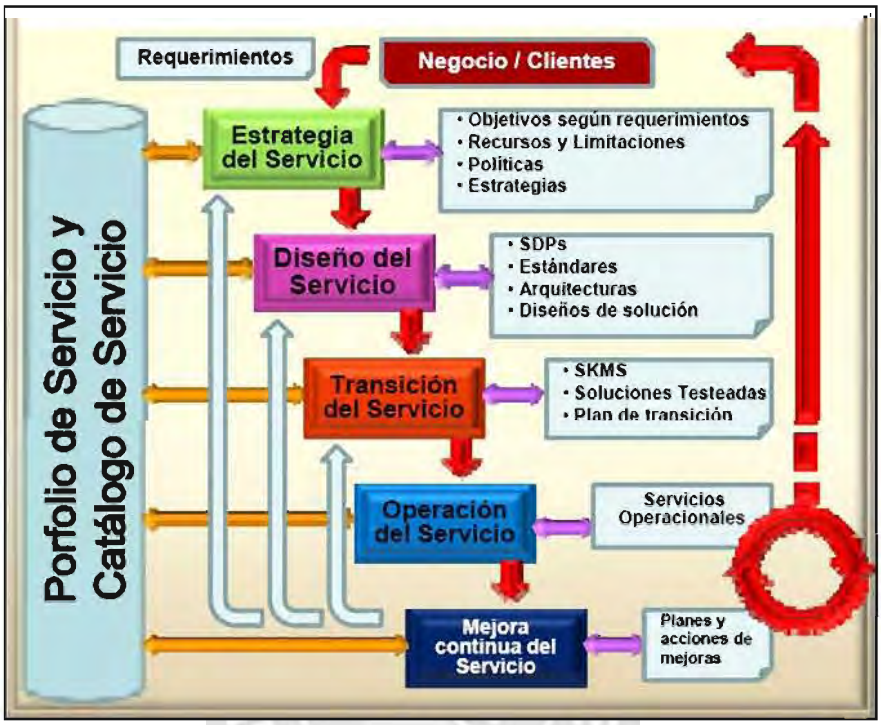


Figura 2: Ciclo de Vida del Servicio.
Fuente: "Fundamentos de Itil V3." Ricardo Adrián Federico.

Estos libros no son departamentos estancos e ITIL tiene en cuenta las múltiples interrelaciones entre ellos y como estas afectan a los aspectos globales de todo el ciclo de vida del servicio. Estos cinco libros ofrecen una guía práctica sobre como estructurar la Gestión de Servicios TI de forma que estos estén correctamente alineados con los procesos de negocio.

2.7.4. Funciones, Procesos y Roles.

ITIL marca una clara distinción entre funciones y procesos.

Una función es una subdivisión de una organización que está especializada en un tipo de trabajo o conocimiento o actividad específica. Son divisiones independientes con capacidades y recursos específicos. Tienen sus propias prácticas y conocimiento

Las funciones tienen como principal objetivo dotar a las organizaciones de una estructura acorde con el principio de especialización. Sin embargo la falta de coordinación entre funciones puede resultar en la creación de nichos contraproducentes para el rendimiento de la organización como un todo. En este último caso un modelo organizativo basado en procesos puede ayudar a mejorar la productividad de la organización en su conjunto.

Un proceso es un conjunto de actividades estructuradas para lograr un objetivo específico.

Los procesos comparten las siguientes características:

- Los procesos son cuantificables y se basan en el rendimiento.
- Tienen resultados específicos.
- Los procesos tienen un cliente final que es el receptor de dicho resultado.
- Se inician como respuesta a un evento.

El Centro de Servicios y la Gestión del Cambio son dos claros ejemplos de función y proceso respectivamente.

Sin embargo, en la vida real la dicotomía entre funciones y procesos no siempre es tan evidente pues puede depender de la estructura organizativa de la empresa u organismo en cuestión.

Otro concepto ampliamente utilizado es el de rol, que lo podemos definir como un conjunto de actividades y responsabilidades asignadas a una persona o un grupo. Una persona o grupo puede desempeñar simultáneamente más de un rol.

Hay cuatro roles genéricos que juegan un papel especialmente importante en la gestión de servicios TI:

- Gestor del Servicio: es el responsable de la gestión de un servicio durante todo su ciclo de vida: desarrollo, implementación, mantenimiento, monitorización y evaluación.
- Propietario del Servicio: es el último responsable cara al cliente y a la organización TI de la prestación de un servicio específico.
- Gestor del Proceso: es el responsable de la gestión de toda la operativa asociada a un proceso en particular: planificación, organización, monitorización y generación de informes.
- Propietario del Proceso: es el último responsable frente a la organización TI de que el proceso cumple sus objetivos. Debe estar involucrado en su fase de diseño, implementación y cambio asegurando en todo momento que se dispone de las métricas necesarias para su correcta monitorización, evaluación y eventual mejora.

2.7.5. Diferencias Entre Versiones V2 y V3.

La principal diferencia entre las versiones v2 y v3 de ITIL es que esta última versión basa su estructura sobre el concepto de Ciclo de Vida de los Servicios.

El Ciclo de Vida del Servicio se compone de cinco fases que se retroalimentan entre ellas de una manera cíclica. [Garcia, 2008].

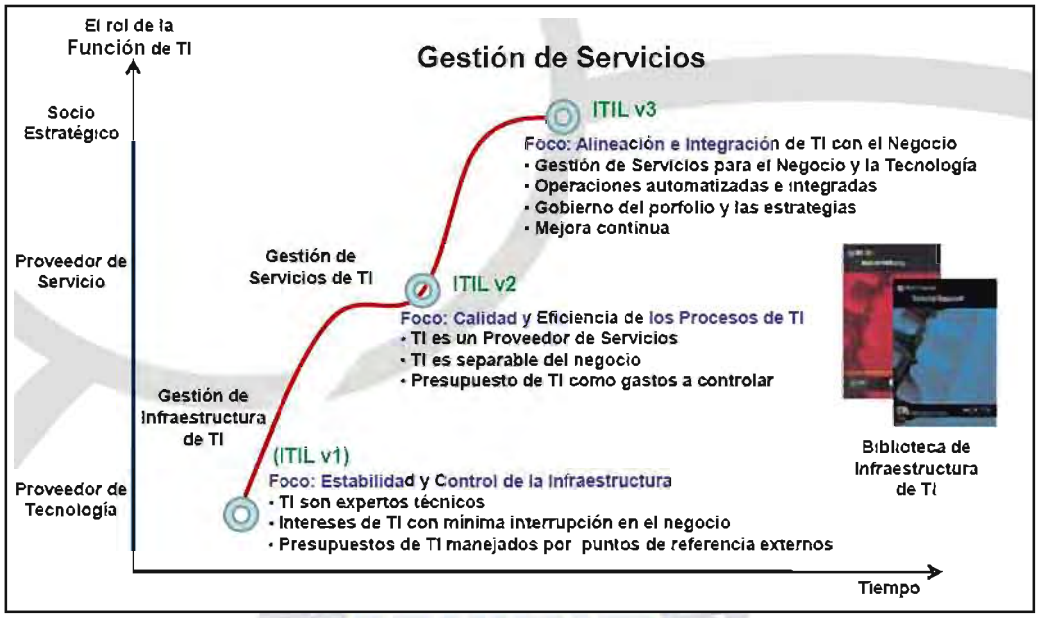


Figura 3: Evolución de Itil.
Fuente: "Fundamentos de Itil V3." Ricardo Adrián Federico.

Los viejos conceptos de Provisión y Soporte al Servicio han sido transmutados en las cinco fases mencionadas párrafos arriba, las cuales se retroalimentan entre si de una manera cíclica.

Sin embargo, ITIL v3 no sólo supone un cambio de perspectiva sino que propone una visión mucho más integral y conceptualmente detallada de todos los aspectos involucrados en la Gestión de los Servicios y sus procesos asociados.

Aunque ITIL v3 continúa orientada a procesos, la relación de éstos con las distintas fases del Ciclo de Vida no es tan rígida como lo era con el enfoque de Provisión y Soporte al Servicio de ITIL v2.

ITIL v3 también introduce como elemento básico el concepto de "función". Un ejemplo de función en el marco de ITIL v2 viene dado por el Centro de Servicios o Service Desk. [García, 2008].

2.7.6. Diferencias dentro el Ciclo de Vida del Servicio para ITIL V3.

Cabe destacar las siguientes principales diferencias en los procesos definidos para ITIL v3: [Business, 2009].

a) Estrategia del Servicio.

- Gestión del Portfolio de Servicios: este proceso encargado de la definición de la cartera o Portfolio de Servicios, incluyendo el Catálogo de Servicios prestados, los servicios retirados y los servicios en preparación, es propio de ITILv3.

b) Diseño del Servicio

- Gestión del Catálogo de Servicios: anteriormente un subproceso de la Gestión de Niveles de Servicio, es un nuevo proceso en ITIL v3 responsable del diseño de un Catálogo de Servicios enfocado a las necesidades de los clientes.
- Gestión de los Proveedores: su principal objetivo es obtener de los proveedores un alto nivel de calidad en su servicio a un precio asequible y adecuado al mercado. En ITIL v2 formaba parte de la Gestión de Niveles de Servicio de los proveedores.
- Gestión de la Seguridad TI: en ITIL v2 se trataba por separado en un libro específico al respecto

c) Transición del Servicio

- Gestión del Conocimiento: este proceso se hallaba subdividido en varios procesos en ITIL v2, como, por ejemplo, mediante la base de datos de errores conocidos en la Gestión de Problemas. En ITIL v3 se ha convertido en un proceso por derecho propio.

- Validación y Pruebas del Servicio: Este proceso se desgaja en ITIL v3 de la Gestión de Versiones o Gestión del despliegue del Servicio para asegurar que se realizan todas las pruebas para validar el servicio como "adecuado en uso y propósito".

- Gestión de la Configuración y Activos del Servicio: Amplía la Gestión de la Configuración de ITIL v2 para incorporar activos no TI.

- Evaluación: exclusivo de ITIL v3, este proceso genérico se ocupa de verificar la relación calidad/precio, el rendimiento y otros parámetros de interés asociados al servicio.

d) Operación del Servicio

- Gestión de Peticiones: se desgaja en ITIL v3 de la Gestión de Incidencias, encargándose de gestionar las peticiones de cambio solicitadas por los clientes.

- Gestión de Eventos: nueva, como tal, en ITIL v3 es la encargada de monitorizar el rendimiento de la infraestructura TI para la prevención de errores o interrupciones en el servicio.

- Gestión de Accesos: es un nuevo proceso en ITIL v3. En ITIL v2 formaba parte de la Gestión de la Seguridad y se encarga de gestionar los permisos de acceso a los diferentes usuarios de un servicio.

Además del Centro de Servicios ITIL v3 introduce nuevas funciones:

- Gestión de Operaciones TI: responsable del mantenimiento de la infraestructura TI.

- Gestión Técnica: responsable del soporte técnico a todos los agentes implicados en la Gestión del Servicio.

- Gestión de Aplicaciones: responsable de la gestión de las aplicaciones de software durante todo su ciclo de vida.

e) Mejora Continua del Servicio

Sus actividades estaban subsumidas por la Gestión de Niveles de Servicio en ITIL v2.

- Proceso de Mejora CSI: establece los protocolos de monitorización, seguimiento y generación de informes y es, en particular, la responsable de generar los Planes de Mejora del Servicio (SIP).
- Informes de servicio: genera los informes sobre rendimiento, resultado y calidad de los servicios ofrecidos.

2.8. ESTÁNDARES DE PROTECCIÓN DE LA INFORMACIÓN.

Se mencionan aquellos que se apeguen a la realización del estándar que se implementara se resumirá a largos rasgos lo más importante de ellos, con el fin de conocer otros estándares que se emplean en diversas empresas aunque estás pueden generar su propio estándar como es para el caso de nuestras entidades u organizaciones.

2.8.1. ISO-15408.

La norma ISO-15408 en 1999, que define estándares de medidas de seguridad TI se implementan en el hardware, firmware o software. La norma ISO-15408 ignora toda medida de seguridad, que esté fuera del dispositivo, para el cual se ha aplicado, aunque reconoce que se puede aplicar seguridad significativa a través del uso de medidas administrativas, como los controles a las organizaciones, al personal, controles de tipo físico y de procedimiento

2.8.2. ISO/IEC 27001.

El estándar para la seguridad de la información ISO/IEC fue aprobado y publicado como estándar internacional en Octubre de 2005 por ISO y por la IEC.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Cic lo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la (BSI).

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) elegido. En general, es recomendable la ayuda de consultores externos.

Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad.

2.8.3. ISO/IEC 27002.

Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la Información se define en el estándar como la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran). [www, 8].

El estándar incluye las siguientes once secciones principales:

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

2.8.4. ISO/IEC 20000

Es el primer estándar específico para la Gestión de Servicios de TI, y su objetivo es aportar los requisitos necesarios, dentro del marco de un sistema completo e integrado, que permita que una organización provea servicios TI gestionados, de calidad y que satisfagan los requisitos de negocio de sus clientes.

La norma proporciona la base para probar que una organización de TI ha implantado buenas prácticas para la gestión del servicio y que las está usando de forma regular y consistente. [Pérez, 2007].

La norma ISO/IEC 20000 está estructurada en dos documentos:

- ISO/IEC 20000-1. Este documento de la norma incluye el conjunto de los "requisitos obligatorios" que debe cumplir el proveedor de servicios TI, para realizar una gestión eficaz de los servicios que responda a las necesidades de las empresas y sus clientes.
- ISO/IEC 20000-2. Esta parte contiene un código de prácticas para la gestión de servicios ("Code of Practice for Service Management") que trata cada uno de los elementos contemplados en la parte 1 analizando y aclarando su contenido. En síntesis este documento pretende ayudar a las organizaciones a establecer los procesos de forma que cumplan con los objetivos de la primera parte.

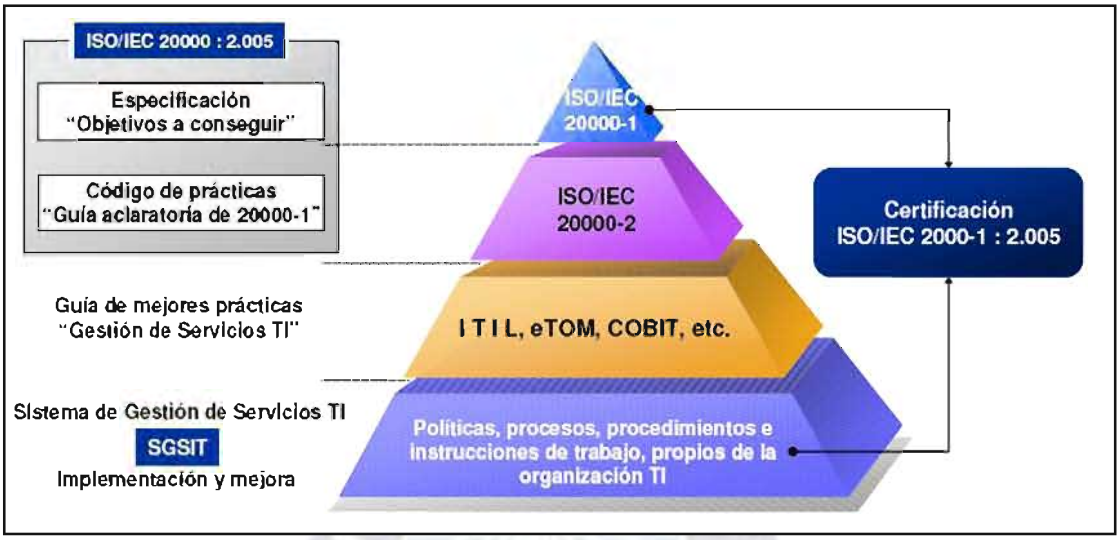


Figura 4: Ámbito de actuación de la norma ISO/IEC 20000.
Fuente: "ISO/IEC 20000 el estándar para la Gestión de Servicios TI." Alejandro Perez.

ISO/IEC 20000 proporciona al sector una norma internacional para todas las empresas que ofrezcan servicios de TI tanto a clientes internos como externos", creando un marco de referencia y una terminología común para todos los actores implicados: los proveedores de servicio, sus suministradores y sus clientes.

En este punto es interesante aclarar que la certificación ISO/IEC 20000 sólo se otorga a organizaciones que realizan operaciones de gestión de servicios TI, y que la norma sólo certifica el buen funcionamiento de esas operaciones, por lo tanto no entran en su ámbito de competencia la certificación de productos, ni servicios de consultoría relativos a la aplicación de buenas prácticas.

Esta norma va dirigida a:

- Organizaciones que busquen mejorar sus servicios TI, mediante la aplicación efectiva de los procesos para monitorizar y mejorar la calidad de los servicios.
- Negocios que solicitan ofertas para sus servicios.

- Negocios que requieren de un enfoque consistente por parte de todos sus proveedores de servicio en la cadena de suministro.
- Organizaciones TI que necesiten demostrar su capacidad para proveer servicios que cumplan con los requisitos de los clientes
- Proveedores de servicio TI para medir y comparar la gestión de sus servicios mediante una evaluación independiente

Como ya se ha mencionado anteriormente, la norma se estructura en torno a la utilización de procesos integrados para la gestión de los servicios TI, posicionándolos en un modelo de referencia y, estableciendo todo aquello que es obligatorio para la buena gestión de los servicios TI.

Estos procesos dan cobertura a las necesidades del ciclo de vida de los servicios, contemplando muchos de los procesos incluidos en la versión 2 de ITIL y otros adicionales, algunos de los cuales fueron posteriormente adoptados por ITIL en su nueva versión 3 publicados dos años más tarde.

La especificación y los requisitos de ISO/IEC 20000 representan un consenso para la industria en estandarización de calidad para la gestión de los servicios TI.

En este apartado se va a tratar cada una de las secciones que forman la norma y sus componentes, reflejando cuáles son sus objetivos y el número de requisitos de control que según la norma deben cumplir.

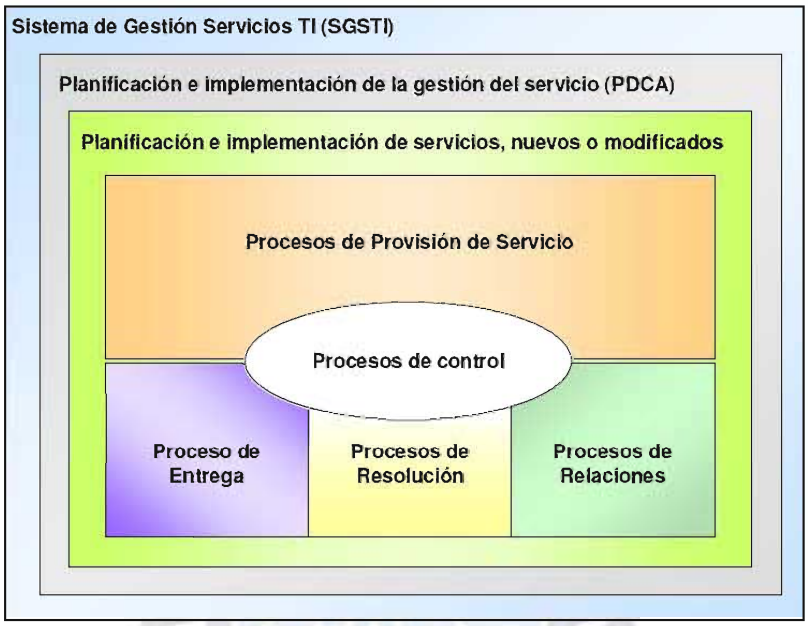


Figura 5: Marco de referencia ISO/IEC 20000.
Fuente: "ISO/IEC 20000 el estándar para la Gestión de Servicios TI." Alejandro Perez.

Es interesante destacar que la norma no enumera sus requisitos de control, por lo que las cifras de reflejadas en este documento pueden variar respecto a otros autores.

Esto es debido a que la norma establece sus requisitos en párrafos, que en algunos casos son "multirequisito", y puede haber autores que consideren solamente estos párrafos. En el caso de esta tesis el número de requisitos se ha establecido, descomponiendo los párrafos con requisitos múltiples en requisitos unitarios. [ISO/IEC 20000, 2007].

2.9. TECNOLOGÍAS EXISTENTES DE PROTECCIÓN.

Como se ha hablado anteriormente de diversos temas, tales como los problemas del por qué se debe de proteger y resguardar nuestra información, nos atañe ahora el conocer las técnicas y medidas, no sin antes ir planteando lo que se tiene por objetivo.

2.9.1. Por que Crear un Respaldo de Nuestros Datos

¿Por qué empezar por este tema? ¿Es necesario tener un respaldo de nuestros datos? Son algunas interrogantes que frecuentemente se preguntaría al leer el encabezado de este tema ya que un respaldo de datos ocupa espacio, por lo cual conlleva a un gasto de recursos que estarán ahí parados sin uso tal vez durante demasiado tiempo.

Una de las cuestiones más importantes al tomar la decisión de la creación de respaldo de datos es la cantidad de dinero que se utilizará y que se va a respaldar; esto sin embargo es lo primero que cualquiera pensaría, pero analizando la situación debemos considerar también los siguientes factores:

a) El tiempo utilizado para recuperar los documentos perdidos o extraviados: Esto es, que tiempo nos tomara el volver a crear nuestro documento. Imagine lo siguiente.

b) El tipo de proceso que se estaba realizando: Para poder entender este punto debe de conocerse el equipo afectado, ya que no es lo mismo que se recupere un servidor a que se recupere el equipo personal de algún trabajador.

En el primer caso, el servidor lleva las transacciones que se realizan con el cliente y entre los mismos usuarios, en caso de un servidor, se tienen los siguientes riesgos:

- Interrupción del servicio de correo interno
- Interrupción de los servicios internos
- Interrupción de las comunicaciones con los clientes
- Interrupción de los servicios al cliente

Todo esto representa pérdidas económicas que van de menos a más.

En el segundo caso, se debe tener en cuenta a cuantas personas afecta que no se tenga a tiempo el trabajo realizado por este empleado, cuanto tiempo de retraso se tendrá y como afectara económicamente a esto.

c) El enfoque de la empresa misma ya que no es lo mismo una empresa que se dedica a servicios de publicidad que una empresa que su negocio está basado en el comercio electrónico, por eso es necesario conocer el giro de la empresa para poder catalogar la importancia de la creación de respaldos.

Es por lo anterior que siempre es bueno tener un respaldo de los trabajos que se están realizando, ya que amortizan el tiempo de recuperación la información que se extravía y es más rápido recuperar un trabajo desde un punto previo a rehacer todo de nuevo.

También es necesario analizar el costo-beneficio de una recuperación, ya que no siempre es más económico recuperar la información perdida a generarla de un backup; un ejemplo claro de esto es la impresión de publicidad en las revistas o periódicos, si estas no están a tiempo, se perdería dinero a gran velocidad, y el tiempo empleado para una recuperación, disminuye las posibilidades de terminar el trabajo de forma correcta y completa, sin embargo el tener un backup o respaldo de este, facilita la culminación del mismo.

2.10. CUELGUES DE SISTEMA, Y COMO PROTEGERSE

Los cuelgues de sistema son uno de los factores más difíciles de solucionar a pesar de que son muy sencillas, ya que detienen por completo el proceso de desarrollo de las actividades que se realizan.

La razón es que cuando ocurre un cuelgue en el sistema, ya sea que deje de responder la aplicación o deje de responder el sistema.

No hay nada que se pueda hacer ante un cuelgue en cuanto a la protección de datos, sin embargo existen diferentes medidas para minimizar estos problemas, y es muy probable que haya utilizado alguna vez, ya que el ejemplo más común es el autoguardado que utiliza Word.

También existen aplicaciones de terceros que generan esta función, en el caso de estas pueden configurarse para que guarden los documentos en algún servidor de archivos que tenga la empresa, esto de manera transparente para el usuario; algunas de estas herramientas son Double Save XT que es exclusiva para el sistema MacOs, o esta Retrospect que genera copias de seguridad pro-activas, es decir genera una copia de seguridad programada en el servidor y generada por el usuario ya que el usuario tendrá que indicar cuándo realizar dicha copia de seguridad al terminar un guardado de documento.

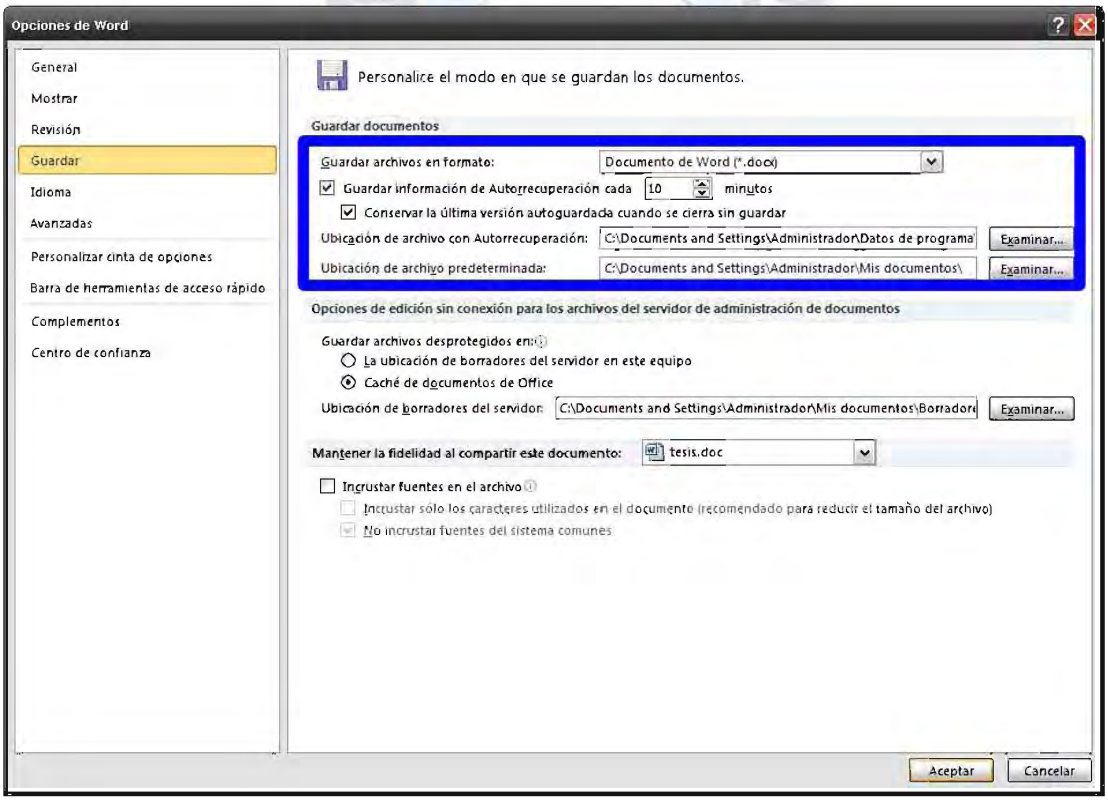


Figura 6: Pantalla para la configuración del autoguardado en office 2010.
Fuente: Elaboración propia.

2.11. PROTECCIÓN CONTRA EL BLOQUEO DEL ORDENADOR.

La diferencia entre un cuelgue y un bloque es que un bloqueo se efectúa sobre el sistema operativo de un ordenador, mientras que un cuelgue es a nivel aplicativo, y este último es posible determinar sin la necesidad de reiniciar el sistema operativo.

Es preocupante este caso en equipos servidores que están funcionando las 24 horas ya que existen momentos en los que no es posible realizar una supervisión de tiempo completo para ellos, imagine que su servidor se cae en un viernes en el que la empresa está celebrando un aniversario más y son casi las 11 de la noche, con este escenario piensa usted que suerte tuvo, sin embargo existe un dispositivo llamado Kick-off, el cual monitorea y reinicia el servidor en caso de ser bloqueado; este dispositivo no solo es un hardware más que se conecta a un puerto USB del servidor, ya que cuenta con un software el cual, monitorea las aplicaciones constantemente preguntando si estas están vivas, en caso de que no reciba respuestas este puede reiniciar la aplicación o si el sistema no responde, reinicia el servidor y pregunta después de la carga del sistema el estado en el que se encuentra, para proseguir con el reinicio de las aplicaciones que se le han configurado para su monitoreo. [Cougias, 2009].

2.12. Corrupción de la información

La corrupción es descrita en el diccionario como el proceso por el cual se altera algo, por ejemplo, si usted maneja una bicicleta tranquilamente y por un descuido se accidenta con un triciclo el cual venía en sentido contrario, y este le pega en la llanta delantera llegando a doblar el rin, este quedara "alterado" o "perdido"; pero si venía a una velocidad en la que el viento golpeaba su cara, es muy probable que tenga que comprar una nueva bicicleta. En esencia la corrupción es una medida de que cosas pueden ser reparadas. Si puede arreglarlo entonces solo esta corrupto, pero si no puede repararlo entonces es que está perdido.

Los documentos, las aplicaciones y los sistemas operativos tienen dos cosas en común. A nivel de ordenador son simplemente archivos, ya que si se analiza el contenido del disco duro lo más probable es que se encuentren carpetas que contienen archivos ya sean de la aplicación de música favorita que use, o de su sistema operativo, sea Windows, Linux, OS X o cualquier otro que se le venga en mente. Esta es la primera cosa que tienen en común.

La segunda y menos agradable es que se pueden corromper a lo largo del tiempo debido a que la aplicación o el sistema operativo se cerraron de forma inesperada. Recuerde esos momentos en los que estaba trabajando alegremente y alguien le apago el equipo de cómputo por jugarle una broma o cuando tuvo una falla eléctrica en casa y se fue la luz...

Estos ejemplos generan fragmentos de datos en algún lugar de su disco, o cuando sufrió de la epidemia de algún virus nuevo que modifico sus documentos, o simplemente algún hacker altero los datos. Llegando a cierto punto, si existe mucha corrupción en un documento se puede producir la perdida de este.

De todas formas la corrupción, es algo que ocurre normalmente con un disco duro. Sin embargo el disco duro no es el único que se puede corromper, también las cintas magnéticas, una prueba de ello es cuando los cabezales lectores no están limpios y se graba con ellas en la cinta, después de varios usos la cinta estará plagada de errores causados por el polvo de los cabezales.

Por último también la red se puede corromper, y dicha corrupción puede afectar a los ordenadores que se conectan a esta. Si está pensando cómo se corrompe una red esto se puede deber a varios factores, entre ellos el uso de un nuevo controlador de cierto proveedor, nuevos grupos de dispositivos de red, o simplemente que se instalen nuevos equipos configurados todos con una misma IP para la administración de SNMP y su administrador no sabe de esto, provocando una enorme tormenta a la hora de resolver las direcciones, entre otras. [Cougias, 2009].

2.12.1. Corrupción de documentos

Como se ha venido mencionando en el capítulo anterior la corrupción existirá mientras tenga uso el equipo de cómputo, sin embargo, en este apartado se tratara la corrupción de los documentos, los cuales contienen la información generada por los empleados de la empresa o de uno mismo. En el uso cotidiano del ordenador utilizamos distintos tipos de archivos: los orientados a aplicaciones y orientados a bases de datos. Los archivos creados por aplicaciones como Excel, PowerPoint, Adobe Creator, entre otros programas sueles abrirse por una sola persona y ser utilizados solo por uno a la vez y en una única maquina. Otros archivos como los generados por Acces, Oracle, Db2, FileMaker o algunos de los creados por aplicaciones de correo electrónico son archivos orientados a bases de datos y por lo tanto pensados para ser utilizados en la red, por múltiples usuarios y que almacenan complejas estructuras. [Cougias, 2009].

La corrupción de documentos puede prevenirse mediante técnicas como la creación de discos espejos, duplicación o replicación. Cualquier dato que pueda ser escrito a un archivo y que pudiese corromperse, será escrito a un archivo espejo o duplicado. Exceptuando la educación que se les dé a los usuarios, que es el punto básico de cualquier prevención, no existen medidas más efectivas.

a) Corrupción de archivos de archivos independientes

Cuanto más grande es un archivo independiente más propenso a corromperse. Este tipo de corrupción en los archivos es causada por que la aplicación se ha cerrado de forma inesperada, dejando trozos de código a lo largo del documento, en lugares en los que no debería.

Sin embargo al ocurrir esto no todo está perdido ya que existen empresas como MicroSystem que han creado herramientas para dar solución a estos problemas. Otra solución para remediar esta situación es hacer copias de seguridad de aquellos archivos importantes que están modificándose con regularidad.

b) Corrupción a nivel de entrada de datos en una base de datos

Los documentos activos de una base de datos son el segundo tipo de documentos. Más allá de las bases de datos corporativas de CRM (Customer Relationship Management) o de gestión de inventario, existen numerosas bases de datos pequeñas a lo largo de la red de la empresa, las cuales crean ruido en el tráfico de la red.

Estas pequeñas bases de datos son mayormente propensas a la corrupción debido a la falta de supervisión por parte del área para su mantenimiento y funcionamiento. En un inicio el uso de este tipo de base de datos, la corrupción suele darse por un error en la red o por que se bloqueó la estación de trabajo, sobre todo cuando se están actualizando los datos.

La única manera de recuperar una base de datos caída es tener una copia de seguridad de la misma y obtener de ella la base de datos tal y como estaba antes de que corromperse, pero tiene un pequeño inconveniente ya que una base de datos tiene los archivos para múltiples usuarios por lo que no es lo mismo que hacer la copia de seguridad de los archivos de un usuario, en estos casos es necesario tener un software capaz de copiar los archivos que estén abiertos mientras se realiza el proceso de copiado.

Algunos programas como Retrospec, NovaStor, Computer Associates y Veritas hacen este tipo de copias de seguridad utilizando parámetros especiales, sin embargo el hacer una copia de seguridad no arreglara el problema, simplemente asegurara que en caso de problemas se contara con una solución viable para poner en marcha nuevamente el servicio.

Aquí se tomaron dos temas, la corrupción en la red y el descuido del usuario, el segundo problema es creado por los usuarios que se conectan a la base de datos y que simplemente apagan su ordenador al pulsar el botón de

apagado, lo cual no solo corrompe a la base de datos del servidor, sino también tiende a corromper los discos duros de los equipos del usuario al mismo tiempo.

El primero esta originado por la corrupción de la red o bien porque el servidor de la base de datos no es el adecuado o está situado en un lugar poco idóneo para este. Para minimizar esto es necesario comprobar la carga de trabajo del servidor. Igualmente tener un servidor de base de datos en un segmento de red corrupto causara problemas en la base de datos así como tenerlo en un segmento de red que no sea adecuado. [Cougias, 2009].

2.12.2. Corrupción del Sistema Operativo

Como se mencionó en apartados anteriores el sistema operativo también se corrompe, si se analiza esta situación, hoy en día, nadie trabaja con el sistema operativo original, ya sea porque se instalaron nuevas actualizaciones del mismo o por que se actualizo algún controlador de los dispositivos que el equipo cuenta, tomando estos detalles y sumando que el sistema operativo también sufre las mimas afectaciones que cualquier otro archivo alojado en el disco duro, podemos decir que sufre igual la corrupción, ya sea por uso del mismo, fallas en la corriente eléctrica, alguna amenaza como los virus, o una infiltración por un ataque externo nos llevan a la corrupción, sin embargo no existe herramienta alguna que cree una copia de seguridad de su sistema operativo más que el reinstalado de las aplicaciones el cual es tedioso y aburrido, sin embargo en capítulos posteriores se tratara la manera más efectiva de cómo "revivir" el sistema operativo mediante diversas herramientas que en más de una ocasión nos han salvado de la tediosa búsqueda de los programas y drivers de los equipos.

2.12.3. Corrupción de los medios de almacenamiento

Recordando que la corrupción es solamente una forma de alteración y descomposición, en el caso de los discos duros esta ocurre como una cosa lógica.

En cualquier caso, debe tener en cuenta cuando las unidades de disco van en camino de corromperse más allá del punto en el que puedan recuperarse.

Hay que tener en cuenta que la corrupción de los medios de almacenamiento es diferente para cada uno de los tipos de medios de almacenamiento, que en general se pueden agrupar en:

- Discos Duros
- Medios electromagnéticos
- Medios Ópticos
- Dispositivos Flash

De las cuales cada una se corrompe de diferente manera.

a) Corrupción de discos duros

Los discos duros son uno de los medios de almacenamiento más empleados, ya que toda computadora los utiliza, así mismo para conocer la forma en que se corrompen, sin embargo son un caso especial ya que existen dos familias importantes, los discos ATA/IDE y los SCSI, sin embargo ambos funcionan de la misma manera.

Un disco duro almacena un archivo en pistas y sectores, las primeras son círculos concéntricos y los sectores son las celdas en que se divide la posta tal y como se puede observar en la siguiente figura.

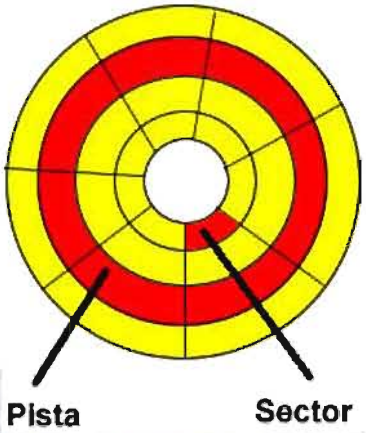


Figura 7: Diagrama de sectores y pistas de un plato de disco duro.
Fuente: Elaboración propia.

El disco duro almacena los archivos en los sectores, y cuando estos son más grandes que el tamaño del sector tiende a fragmentar el archivo colocándolo en sectores contiguos, pero esto no siempre es así ya que al existir archivos con tamaños diferentes estos hacen que el disco duro los almacene en cualquier sector disponible, el cual apunta al siguiente sector que contenga la información correspondiente al archivo, esto se conoce como un archivo fragmentado, sin embargo el disco puede estropear de manera física esta área ya que al estar compuesto de discos que giran a altas velocidades y agujas lectoras, que se conocen como cabezales, pueden producir ciertas irregularidades en la superficie del disco cuando ambas llegan a rozar, así mismo el polvo genera alteración en la lectura disminuyendo el rendimiento, sin embargo existen utilidades como Norton Disk Doctor que revisa y "repara " estos errores.

Se dice que estas utilidades arreglan las unidades de disco duro, pero lo que realmente hacen es bloquear los sectores defectuosos y modificar el contador de sectores, esto a su vez degrada el rendimiento de la unidad ya que hace menor el espacio disponible en el disco duro, por lo tanto después de verificar un disco debe comprobar que hay suficientes pistas disponibles que permitan aislar los bloques defectuosos para su reparación.

Se ha mencionado el cómo almacenan los discos los archivos los cuales no son necesariamente secuenciales, sin embargo por el uso constante de las máquinas y el guardado de los archivos que se modifican, crean y borran, el disco va almacenando espacios huecos en los cuales deposita fragmentos del archivo, esto no es en sí de todo malo ya que es la forma en que trabaja el disco duro, sin embargo a la larga puede producir corrupción de los datos almacenados y un rendimiento menor en el disco duro debido a los accesos al mismo haciendo que se vuelva más lento.

Es por eso que la fragmentación no es necesariamente un sinónimo de corrupción pero si se descuida esto puede producir problemas graves. Sin embargo existen aplicaciones que permiten desfragmentar los discos, tales como Drive10 para sistemas OsX , DiskKEeper, Tune Up, entre otras las cuales ayudan a la desfragmentación del disco sin embargo en los sistemas Unix y Windows existe de forma nativa.

Estas herramientas se deben de utilizar cada vez que se depura el disco duro, es decir, cada vez que se borra una gran cantidad de archivos, también cuando se instalan o desinstalan programas ya que como se mencionó estos también son compendios de archivos que hacen que se ejecute una aplicación.

Sin embargo en los servidores de archivos es necesario realizar una desfragmentación en relación a su uso diario, es decir mientras más uso tenga un servidor más pronto requerirá una desfragmentación del disco, en especial si se trata de creación, modificación y borrado de archivos, lo más recomendable es que se realice un análisis del disco duro semanalmente y hacer caso a la indicación de la aplicación para mantener el rendimiento óptimo del sistema.

2.12.4. Herramientas para revisión de discos.

a) DRIVE10 (Os X)

Esta herramienta es para el mercado de los equipos Mac Os X de la empresa de Micromat. La cual ha sido utilizada para comprobar los efectos que tiene la microgravedad en los equipos electrónicos por la NASA en un vuelo.

Tiene una elegante interfaz, este producto es para la reparación y recuperación avanzada de discos y ha sido diseñado en exclusiva para entornos Mac Además de reparar unidades y recuperar datos, proporciona la capacidad de hacer copias de seguridad automáticas a intervalos regulares, de estructuras de datos importantes.

b) Diskeeper Server y Workstation

Esta herramienta de Exclusive Software se distribuye en dos versiones, la de servidor y la de estación de trabajo. Con esta combinación de productos el administrador de red puede gestionar el calendario de implantación de un sitio con unos clics, permite establecer un calendario para los análisis y desfragmentación de los archivos, el cual nos permite establecer con qué frecuencia se realizara, los volúmenes a desfragmentas y los equipos de red en la versión servidor todo esto con unos cuantos clics también y de manera muy intuitiva

2.12.5. Corrupción en la red.

La corrupción en la red física se debe a tres puntos básicos:

- Un mal cableado realizado por el instalador de la red, dejando cables donde cualquiera puede dañarlos y en el peor de los casos dejar nula la conectividad de los equipos a la red
- Exceso de routers en la red, los cuales ralentizaran la comunicación por el exceso de búsquedas de direcciones.

- La mala planeación de la actualización de la red, olvidando migrar a toda la tecnología existente, lo cual provocará cuellos de botella haciendo que la comunicación de datos se vea interrumpida o mezclada.

Esto genera una mala transmisión en los datos dando lugar a intermitencias o caídas en el servicio, o que la información llegue con muchos errores y ralentice la red.

La corrupción de la red a nivel datos se da también por esos motivos sin embargo existe un factor más que afecta a esta; el cual es el uso excesivo de aplicaciones que usen la red, ya que generaran nuevos paquetes creando una saturación en la red, logrando así que llegue inconclusa la información que se envía.

Otro posible problema es que el paquete no sea enviado correctamente y se tenga que reenviar el mismo, lo cual incrementa la cantidad de información, llegando a colapsar las redes cuando esta se vuelve excesiva.

La solución en estos dos casos es sencilla y simple ya que se deben tomar las siguientes medidas preventivas:

- Revisar el cableado periódicamente, en especial si se actualiza la tecnología empleada en ese momento
- Verificar que la planeación de una actualización cumpla con lo necesario para su buen funcionamiento

Estas soluciones solo pretenden minimizar la corrupción y pérdida de información.

2.13. SEGURIDAD PERIMETRAL EN LAS ENTIDADES.

El objetivo de este tema es identificar los puntos clave para mantener una seguridad en la red empresarial y en la física; lo cual hará que se piense inmediatamente en hackers externos que son genios en seguridad, que hasta cierto

punto es y será cierto, sin embargo existe un grupo de estos el cual es más peligroso, y este está dentro de las instalaciones de la empresa.

Se vuelve más peligroso porque este grupo conoce las debilidades de la seguridad en la empresa, sin embargo, se puede empezar a proteger la red por la colocación de un firewall, lo cual limitara el acceso de los externos.

Si usted cree que un firewall detendrá a todos sus intrusos, debe tener en cuenta que este puede fallar, a pesar de que sea un firewall de hardware o por software, ya que los intrusos pueden entrar por la puerta y llevarse algún equipo con un mínimo de fuerza utilizando la ingeniería social, la cual ha sido el método más utilizado por un hacker. Hay quienes llegan a considerar la ingeniería social como un arte ya que les permite actuar papeles que no lo son, y manipular a los demás.

Sin embargo, también es necesario administrar la red, ya que si no se controla esta se tiene un descontrol de los datos que circulan, una cuestión importante es el mantener un mapa de la red y mantener solo los nodos necesarios activos, imagine que su empresa da una conferencia publica y una persona sin intenciones lleva su equipo de cómputo, se conecta a la red sin que esté autorizado, y husmea delante de sus narices por toda la red, llegando a bloquear la misma. Un ejemplo de este caso esta descrito en el libro "el arte de la intrusión" en el cual se describe como un equipo de auditores simula un ataque a la red y coloca un dispositivo inalámbrico en un nodo al cual tenían acceso en la sala de espera de la empresa, obteniendo así el acceso a la red... En este caso fue una prueba de penetración que dio una lección a la empresa y demuestra que puede ocurrir.

En estos casos la mejor manera de proteger los perímetros de nuestra red es mediante el uso de diversas herramientas, entre ellas hay algunas que nos permiten comprobar las vulnerabilidades de la red.

2.13.1. Herramientas para Comprobar la Red.

a) NetRecon

Esta herramienta de Symantec utiliza un motor de análisis de causa y caminos posibles para mostrar los pasos que se toman para destapar las vulnerabilidades. Comprueba toda la red con el fin de localizar vulnerabilidades de seguridad y proporciona recomendaciones de cómo repáralas.

b) Nessus

Esta herramienta es un proyecto de código abierto lo cual tiene su beneficio, ya que hay una gran cantidad de soporte y dispone de una arquitectura abierta, esta arquitectura hace que se base en componentes. Cada prueba de seguridad está escrita como un complemento externo, de forma que pueden añadírsele módulos que permiten la personalización de sus comprobaciones.

Nessus Security Scanner incluye su propio lenguaje el cual está diseñado para la escritura de pruebas de seguridad de forma fácil y rápida.

2.13.2. Firewall.

Los firewalls son barreras que actúan principalmente de seguridad, regulando el tráfico entre los puertos estableciendo reglas, las cuales son: aceptar tráfico en puertos determinados, ignorar tráfico en puertos establecidos, redirigir el tráfico que llegue a puertos establecidos y restringir servicios que los usuarios deseen acceder mediante la red. Un firewall proporciona pocas ventajas de seguridad para redes corporativas/empresariales, ya que solo actúa como una alarma para el tráfico de la red, generando registros de información sobre sucesos ocurridos en los puertos.

Estos firewalls están conformados como tipo software o hardware, visto de una mejor forma un firewall puede ser un router, una computadora que mantiene la red (servidor) o una computadora en específico (host), ambas con el fin de mantener una información al día sobre los movimientos o sucesos obtenidos en la comunicación

entre equipos mediante sus puertos. Para una mejor comprensión veamos la figura.

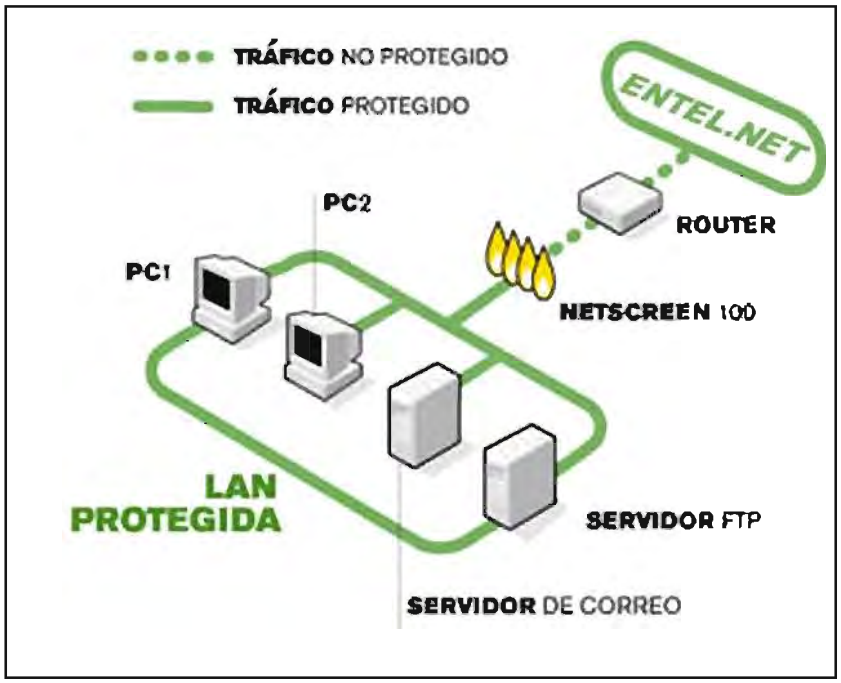


Figura 8: Se observa como un firewall protege la red atreves de puertos.
Fuente: Elaboración propia.

Para implementar el firewall se puede hacer de tres formas:

- Firewall de red basado en host. Es un equipo que actúa como firewall entre la Intranet e Internet.
- Firewall basado en host. Es un firewall que actuará por equipos, y estará instalado en cada equipo. Ejemplo: ZoneAlarm, Kerio, etc.
- Firewall basado en routers. Es el firewall del router con el cual a través de políticas se protege la red.
- Firewall de equipos. Es el firewall interno que tienen los dispositivos de hardware y son configurables mediante el mismo

sistema operativo o bien el software que proporciona el fabricante al instalar el controlador.

2.13.3. Detectores de intrusos.

Se ha hablado de la delimitación del acceso mediante firewalls los cuales llegan a ser insuficientes ante las destrezas de los atacantes ya sea interno o externo, en otros casos, suele pasar que el firewall confunde accesos ciertos con intentos de ataque por lo que es necesario distinguir estos de los ataques que se realizan a la red empresarial.

Existen programas como Snort que sirven para la detección de intrusos, este tipo de software analiza los paquetes de red escaneando cada uno de ellos y diferenciando los ataques repetitivos descubriendo así a un atacante de una solicitud repetitiva.

Otra de las herramientas de detección de intrusos es Whireshark antes conocido como Ethereal el cual es libre y se encuentra para distribuciones Windows y Linux, lo cual le permite un soporte más extensos, y permite analizar redes alámbricas e inalámbricas, en Windows, estos programas necesitan un driver conocido como Winpcap, el cual les permite esta funcionalidad.

2.13.4. Unificando las técnicas.

Anteriormente se han mencionado diferentes técnicas para proteger los datos y contra que se están protegiendo, pero estas técnicas deben de estar contenidas en un plan o algún manual que la empresa tenga.

A este manual se le conoce como plan de contingencia, el cual algunas veces es desconocido por el personal de soporte técnico o no es un plan integral de contingencia ya que solo contempla algunos aspectos generales, pero no específica que hacer en casos diarios, sin embargo existe.

El peor escenario es cuando no existe dicho plan ya que deja indefensa a la empresa en caso de cualquier percance natural, si se cuenta con este se tiene una

idea de que hacer en un sismo, que hay que hacer si se incendia el cuarto donde residen los servidores.

Desgraciadamente no existe herramienta alguna, que genere estos planes de contingencia ya que se deben de considerar las variables que existan en estos momentos como son el clima de la región, el factor político de la región, la ubicación geográfica y las mismas políticas empresariales.

2.14. RESPALDO DE ARCHIVOS.

Los sistemas de respaldo (backup) y los sistemas redundantes son dos técnicas para proteger los datos contra pérdida por borrado accidental o desastres fortuitos. Ambos sistemas son complementarios en cuanto a la seguridad que ofrecen ya que tanto los respaldos como la redundancia, por si solos, no cubren toda la necesidad.

2.14.1. Redundancia: los sistemas RAID.

Un RAID es un conjunto de unidades de disco que aparecen de forma lógica como si fueran un solo disco. Así los datos, distribuidos en bandas, se dividen entre dos o más unidades.

Esta técnica incrementa el rendimiento y proporciona una redundancia que protege contra el fallo de alguno de los discos de la formación.

Existen varios niveles RAID a partir del nivel 0, en el que los datos se dispersan en varias unidades pero no hay redundancia (gran rendimiento pero la seguridad es nula). Luego el nivel 1 o mirroring (espejo) en el cual los datos se escriben duplicados en distintas unidades, este método no incrementa el rendimiento pero si la seguridad y es, de hecho uno de los más utilizados.

EL nivel 5 usa división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos miembros del conjunto. El RAID 5 ha logrado popularidad gracias a su bajo coste de redundancia. Generalmente, el RAID 5 se

implementa con soporte hardware para el cálculo de la paridad. Generando así un mayor rendimiento y seguridad en la escritura de los datos; sin embargo es más costosa que la implementación de RAID nivel 1. La duplicidad de los datos siempre debe ser en discos distintos.

2.15. TECNOLOGÍAS EXISTENTES DE RECUPERACIÓN DE DATOS.

Existen muchas herramientas en el mercado así como métodos implantados por especialistas en el ámbito laboral que tienen la finalidad de recuperar el máximo de información posible ante un incidente determinado. Una de las formas de recuperación más utilizada es para los discos duros.

También es posible recuperar datos de otros medios, como por ejemplo, memorias flash de todo tipo. Además medios de almacenamiento óptico y magneto-ópticos que también son dispuestos de que por lo menos intentemos la recuperación.

Hay que tener en cuenta que la recuperación debe de ser controlada con el único propósito de salvaguardar nuestra información para ser reutilizada ya que no siempre es así, hay quienes utilizan estos métodos y herramientas con fines ilícitos o personales.

2.15.1. Métodos de Recuperación de Datos.

Los problemas con el hardware, con frecuencia son causados por errores humanos: un 30% de los casos. Presionar "sin querer" la tecla de suprimir o copiar encima de un fichero, los actos malintencionados de empleados descontentos. Seguidamente, un 15% de las pérdidas de datos se deben a disfunciones del software, un 7% a los ataques de virus y menos del 4% estarían provocados por catástrofes naturales.[www, 9]

a) Información borrada manual o intencional.

Un archivo al ser borrado por el usuario accidental o intencional puede ser mandado a la papelera de reciclaje o bien eliminado directamente sin pasar por ella.

Al pasar directamente a esta el procedimiento a seguir para recuperar la información es:

- En el escritorio dar clic derecho sobre el icono bandeja de reciclaje.
- Al estar dentro de esta dar clic derecho sobre los archivos deseados, eligiendo la opción de restaurar.
- Esta información al ser restaurada va a regresar a la carpeta de donde se borró.

Pero cuando la información es borrada directamente sin pasar a la papelera de reciclaje o eliminada de esta no desaparece totalmente aunque el usuario no lo pueda ver, ya que estos aunque estén eliminados pueden recuperarse bajo ciertas condiciones cuando se van a esta.

En algunas ocasiones un archivo puede recuperarse completo o sólo partes, todo depende de si fue o no reemplazado físicamente en el disco duro por otra información. Ya que hay usuarios que sin querer a la hora de guardar no se dan cuenta de que lo están remplazando.

Lo ideal sería darse cuenta enseguida que se han eliminado archivos que son importantes. A partir del momento que han sido eliminados, si se sigue utilizando ese disco duro, la información de los archivos borrados puede ir perdiéndose de a poco a medida que es reemplazada por otra información. Por lo tanto es importante dejar de usar el disco duro en cuestión hasta no ser recuperados.

Lo más recomendado sería poseer un segundo disco duro (configurado como maestro), donde debe estar el sistema operativo, y así poder acceder al otro

disco duro donde se encuentra la información que se desea recuperar (configurado como esclavo) para poder recuperarla.

Igualmente existen programas más efectivos, que no necesitan instalación y pueden ejecutarse directamente desde un disquete o CD y, de esta manera, se evita utilizar el disco rígido que posee los archivos eliminados, minimizando los riesgos.

b) Recuperación de los archivos borrados.

Para recuperar los archivos perdidos necesitaremos un programa especial que lo haga. En el mercado existen decenas de este tipo de programas tanto gratuitas o compradas.

Si posee ese segundo disco duro con Windows o instaló su disco en otra computadora, debe proceder a instalar el programa de recuperación de archivos.

Una de las mejores herramientas en el mercado es "Restoration 2.5.14", ya que es un muy buen recuperador de archivos. La mayoría de estos programas son muy parecidos entre sí, así que se pueden utilizar otros también. Como se dijo anteriormente, este programa permite funcionar sin ser instalado, por lo tanto puede copiarse a un disco (CD, disquete, DVD) y ejecutarse directamente desde allí.

Al abrir el programa desde "Restorarion.exe", podemos ver que es sumamente sencillo, sin demasiadas opciones. A la derecha, en "Drives", se encuentran los distintos dispositivos de almacenamiento, se deben de elegir cuál es el que posee los archivos que se desean recuperar.

Inmediatamente abajo se encuentra un campo de búsqueda, allí va el nombre o parte del nombre del archivo a recuperar.

Por ejemplo: Si se necesita recuperar un archivo llamado documento.doc, simplemente se tiene que escribir en el campo de búsqueda: documento.doc; en caso de necesitar un lista de los archivos de texto eliminados podemos buscar "txt" en el campo de texto.

Si el archivo o los archivos han sido encontrados, se mostrarán en la lista. Se deben seleccionar y presionar el botón de la derecha "Restore by copying" y seleccionar la carpeta donde se restaurarán. Lo recomendable sería elegir una carpeta que no esté en el mismo disco duro desde donde se están recuperando los archivos, o sea, en otro disco duro de la PC, o directamente hacia un disquete.

Lamentablemente, es imposible garantizar una recuperación 100% efectiva de los archivos que han sido eliminados, por eso, la mejor manera de no tener que pasar por una situación de estas características, es mantener un respaldo (backup) de nuestra información más importante.

c) Recuperación del Sistema Operativo

Debido a virus, cortes en el suministro eléctrico que ocurren por no tener la debida supervisión del ciclo de vida de estos y gente malintencionada unos de los aspectos importantes para la pérdida de datos son los sistemas operativos tanto en servidores como en los equipos de cómputo de los usuarios de la empresa.

En tanto a los virus que dañan el sistema operativo, no están fácil repararlo aunque se sustituya el archivo que se dañó dependiendo el tipo de virus que lo ataco. Existen tres opciones: restaurar el sistema desde el disco que se instaló, desde una copia de seguridad y creando una imagen y opciones que te da el sistema operativo.

- **Métodos para el Sistema Operativo**

Estos métodos son muy importantes ya que la mayoría de los virus atacan principalmente al sistema operativo es significativo conocer cuales se encuentran en la actualidad para en caso de ocurrir algún desastre tener las herramientas suficientes para minimizarlo.

Estas herramientas que se describen a continuación son las más conocidas e importantes para que el usuario salve sus datos.

- **Servidores**

El primer caso mencionado anteriormente la restauración del sistema es un proceso largo y tedioso debido a que una vez cargando los discos, se tienen que bajar actualizaciones desde internet y sucesivamente configurar el sistema pero no deja de ser un método factible para la recuperación.

Con la copia de seguridad es el método más fácil de incorporar en la planificación de copia de seguridad de la organización, pero probablemente no haya establecido un plan para admitir la restauración paralela en vez de la restauración lineal. [Cougias, 2009].

Cuando se realiza la restauración del sistema de una cinta a un computadora para la mayoría de la gente es suficiente, pero hay que tener en cuenta que si el virus ataca a la mayoría de las computadoras de la empresa. El uso de la restauración lineal de muchas computadoras necesita mucho tiempo.

Cuando se dispone de una herramienta que admita la recuperación paralela, se ahorra crear un disco ERD y así crear un solo disco de arranque para que cada computadora arranque contra un software basado en Intranet que pueda conectarse al servidor en copia de seguridad y así se lleve a cabo la restauración.

En el caso de no contar con una herramienta para la restauración paralela se proseguirá al tercer paso mencionado creando una imagen de una unidad predeterminada para poder clonar muchas de las computadoras como se mencionó en el tema de métodos y herramientas de protección de datos, con lo resultados obtenidos de los métodos anteriores se proseguirá a la restauración del sistema y con ello la obtención de datos.

- **PC**

Al igual que los servidores en las computadoras hay opciones para poder recuperar el sistema operativo y así obtener los datos.

Anteriormente se explicó que una de las soluciones era tener el CD original con el que se instalo y por medio de este restaurarlo siguiendo a continuación los pasos:

- **Restauración de sectores y reemplazo de disco duro**

La restauración de un disco duro no borra ni sobrescribe la información contenida en el disco duro y no depende de ningún sistema de archivos tales como NTFS, FAT, HFS, HFS+, etc. Su único fin es el de permitirle a la computadora el poder leer y escribir nuevamente en los sectores que tenían errores. Por esta razón, se utiliza esta técnica para la "recuperación de información" o para el respaldo de la misma.

Los discos duros tienen sectores dañados o defectuosos desde que son ensamblados por su fabricante. Dichos sectores son marcados como "defectuosos" para evitar que sean utilizados. A este proceso se le conoce como "calibración", y la información resultante del mismo es almacenada en la tarjeta lógica del disco duro. Cada disco duro, aunque sea de la misma marca y modelo, tiene una calibración única.

En cuanto al reemplazo es en el caso de que el disco sea inservible por tal motivo es importante conocer técnicas para la restauración y reemplazo de este.

2.15.2. Herramientas de recuperación de datos borrados y dañados

Existen diferentes herramientas para distintos dispositivos donde se encuentra almacenada la información, ya que la gente en muchas ocasiones no tiene el debido cuidado para respaldar y mantener está a salvo o muchas veces esta información es ocupada para fines ilícitos. Se mencionaran algunas de las herramientas existentes de tipo: Gratis y Shareware.

a) Disco duro

Se encuentran herramientas especializadas para recuperar datos de discos borrados o inutilizados, la necesidad de recuperar datos alcanza a todos los humanos que usan ordenador.

Ya sea porque un virus ha destruido la FAT (File Allocation Table) o el MBR (Master Boot Record), porque se ha formateado accidentalmente el disco duro, eliminado archivos o porque un fallo de funcionamiento del sistema operativo o del dispositivo ha corrompido la información de acceso al disco.

2.15.3. Herramientas para Sistema Operativo LINUX

a) Get Data Back for Linux

Recupera archivos de Linux y restaura datos mediante pasos sencillos usando las mejores herramientas de recuperación de datos para Linux. Recupera fácilmente archivos Linux de discos rígidos de Linux formateados, corrompidos, dañados o inaccesibles. El programa Get data back for Linux es una aplicación basada en Windows para recuperar datos de Linux, que se instala completamente en el sistema operativo Windows y realiza la recuperación de discos rígidos Linux.

El programa recupera perfectamente archivos eliminados con las teclas Mayúsculas+Suprimir (shift+delete) de discos rígidos Linux. Es de Tipo: Shareware.

b) R-Linux Data Recovery Utility

R-Linux es una utilidad de software de la recuperación de los datos, undelete la herramienta para el sistema de ficheros de Ext2FS (Linux). Archive la recuperación después del apagón, fallo del sistema, infección del virus o la partición con los archivos fue cambiada formato. Es de Tipo: Shareware.

2.15.4. Herramientas para Sistema Operativo XP

a) HDD Data Recovery Software

HDD Data Recovery Software diseñado para recuperar archivos de unidades de disco duro desde unidades de disco duro de Windows. Tiene herramientas de recuperación de datos de unidades de disco duro para recuperar los datos desde unidades de disco duro formateadas.

Software de recuperación de datos de unidades de disco duro para recuperar datos desde unidades de disco duro incluso después de tener sectores dañados en la unidad de disco duro. Elsoftware de recuperación de unidades de disco duro de Windows recupera de forma sencilla los archivos eliminados cuando la tabla de particiones ha sido dañada. El software de recuperación de datos de unidades de disco duro o programa de recuperación de archivos de unidades de disco duro recupera de forma sencilla los archivos eliminados incluso si los MBR, MFT y FAT han sido corrompidos. Es de Tipo: Shareware.

b) EasyRecovery Professional

- Solución completa para sus necesidades de recuperación de datos
- Incluye funciones de EasyRecovery DataRecovery, EasyRecovery FileRepair yEasyRecovery EmailRepair
- Además de opciones avanzadas de recuperación de datos y funciones de diagnóstico de Data Advisor®
- Funciones generales: recuperación de datos, reparación de archivos, diagnóstico de discos
- Funciones de recuperación: cualquier tipo de sistema operativo y medio de Almacenamiento

- Funciones de reparación de archivos: Microsoft Outlook (PST, OST), Outlook Express (DBX), Word (DOC), Excel (XLS), bases de datos de Access (MDB), PowerPoint (PPT) y Zip (ZIP). Es de Tipo: Shareware.

c) Getdataback

Es una herramienta de recuperación de archivos, capaz de recuperar los datos perdidos tras una infección de virus, un fallo general del sistema, un problema grave con el disco duro o un simple borrado accidental.

Puede recuperar los archivos de un disco duro incluso aunque Windows no lo reconozca como unidad, o se haya perdido toda la información de estructura de directorios. Es fácil de usar, gracias a su sistema de recuperación dividido en cinco pasos que te vaindicando qué hacer en cada momento. GetDataBack utiliza avanzados algoritmos para garantizar la recuperación total y correcta de archivos y directorios.

El programa viene en dos versiones, una para sistemas de archivos FAT y otra para sistemas NTFS, y también permite recuperar unidades a través de red local o con un cable serie. Es de Tipo: Shareware.

d) Salvage Files Data Recovery Software

La aplicación Salvage Files Data Recovery Software ofrece un amplio rango para restaurar la información y herramientas para recobrar archivos y así poder regresar los archivos borrados desde el SO Microsoft Windows. Nuestra herramienta Salvage Files Data Recovery Software utiliza técnicas avanzadas que le permiten recuperar y restaurar esos archivos borrados. Los datos, archivos y contenidos de los programas de Microsoft como el Word, Excel, PowerPoint, Access y MS Publisher, los archivos con formato PDF de Adobe Acrobat pueden ser recuperados de una forma efectiva y restaurados a una ubicación, utilizando el programa Salvage Files Data Recovery Software. Es de Tipo: Shareware.

e) Data Recovery Software

Data Recovery Software es una herramienta profesional de recuperación de archivos para Windows que recupera archivos / carpetas eliminadas desde un disco duro con Windows que haya sido borrado o formateado. Advanced Data Recovery Software es una herramienta poderosa de recuperación de datos para recuperar datos eliminados desde la partición de Windows (FAT - NTFS), basada en Windows 98/ME/NT/2000/XP/2003/Vista. Data Recovery Tool es para recuperar y restaurar los máximos datos posibles desde el sistema corrupto de archivos de Windows. Es de Tipo: Shareware.

f) Recover Files

Recover Files es un laureado programa que sirve para recuperar archivos después de que hayan borrados del disco duro.

Se trata de una herramienta profesional cuya fiabilidad y eficacia han sido ya más que demostradas. Es capaz de recuperar datos eliminados de la papelera de reciclaje, de unidades de red, tarjetas de memoria, tarjetas Compact Flash, unidades extraíbles, dispositivos portátiles, etc.

También restaura las fechas originales de creación y modificación de cada archivo.

Recover Files es pequeño (ocupa poco más de un megabyte), rápido, funcional y muy práctico. Te puede librar de más de un disgusto. Funciona en cualquier plataforma Windows, y en particiones formateadas con NTFS o con FAT. Es de Tipo: Gratuito

g) Recuva

- Recupera archivos aunque la papelera de reciclaje haya sido vaciada
- Recupera imágenes y otros archivos que han sido eliminados de memorías SD, MMC, Memory Stick, XD de cámaras, reproductores de MP3, etc.

- Recupera archivos que han sido eliminados por virus y errores del sistema.

Soporta medios con sistemas de archivos FAT12/16/32, NTFS/NTFS5. Es de Tipo: Gratuito.

h) Undelete Plus

- Recupera archivos aunque la papelera de reciclaje haya sido vaciada
- Recupera archivos que han sido eliminados permanentemente de Windows usando Shift + Delete
- Recupera archivos que han sido eliminados desde la línea de comandos (terminal, MS- DOS).
- Hace una imagen de recuperación de tarjetas Compact Flash, SmartMedia, Multimedia y Secure Digital.

Soporta medios con sistemas de archivos FAT12/16/32, NTFS/NTFS5. Es de Tipo: Gratuito

i) PC INSPECTOR File Recovery 4.x

- Encuentra particiones automáticamente, incluso si se ha borrado o se ha dañado el sector de arranque.
- Recupera archivos con todos los atributos originales de la fecha de creación y todo eso.
- Soporta la opción de guardar los archivos recuperados en una unidad de red.
- Recupera archivos, incluso si su encabezado no está disponible. Con la función "Special R ecovery Function" soporta los siguientes formatos: ARJ AVI BMP CDR DOC DXF DBF XLS EXE GIF HLP HTML HTM JPG LZH MID MOV MP3 PDF PNG RTF TAR TIF WAV y ZIP.

Soporta medios con sistemas de archivos FAT 12/16/32 y NTFS. Es de Tipo: Gratuito.

j) Glary Undelete

- Recupera archivos aunque la papelera de reciclaje haya sido vaciada o hayan sido eliminados desde una ventana de MS-DOS o usando Shift + Delete.
- Recupera archivos que han sido eliminados por virus y errores del sistema.
- Recupera archivos de dispositivos extraíbles cómo (SmartMedia, Secure Digital, MemoryStick, etc.). Es de Tipo: Gratuito.

k) NTFS Undelete

- Recupera archivos directamente del disco duro aun habiendo vaciado la papelera de reciclaje.
- Puedes crear un disco (CD, DVD) de arranque para tratar de recuperar desde ahí los archivos.

l) PhotoRec

- Recupera archivos suprimidos incluyendo video, documentos y archivos desde el disco duro CD-ROM y fotos eliminadas de una cámara o teléfono celular.
- Trabaja incluso si el sistema de archivos de tu disco duro se ha dañado o se ha cambiado el formato seriamente Soporta medios con sistemas de archivos FAT, NTFS, EXT2/EXT3 filesystem, HFS+. Es de Tipo: Gratuito.

m) R-Studio Data Recovery Software

- Herramienta de la recuperación de los datos para los sistemas de ficheros FAT, NTFS, Ext2FS/Ext3FS y UFS1/UFS2. Archive la recuperación

después de FDISK, destrucción de MBR, FAT dañado, infección del virus. Reconstrucción dañada de la INCURSIÓN. Es de Tipo: Gratuito.

n) EasyRecovery FileRepair

- Repara y restaura archivos dañados o inaccesibles de Microsoft® Office y archivos Zip, convirtiéndolos en archivos legibles.
- Funciones generales: reparación y restauración de archivos.
- Funciones de reparación de archivos: Word (DOC), Excel (XLS), bases de datos de Access (MDB), PowerPoint (PPT) y Zip (ZIP).

2.15.5. Memorias extraíbles

a) Undelete Thumb Drive

Sirve para la recuperación de datos en unidades del tipo USB puede de una forma muy sencilla traer de vuelta archivos que hayan sido borrados o eliminados desde cualquier medio de almacenamiento con interfaz USB que haya estado conectado a su computadora. El programa de recuperación de datos en medios removibles realiza un análisis completo de la unidad Pen Drive para buscar rastros de archivos perdidos y de esta forma le permitirá al usuario realizar una pre visualización de ellos en el mismo estado en que fueron encontrados.

La herramienta para recobrar del formato unidades Pen Drive puede recuperar sus archivos musicales en MP3, archivos de video, imágenes, fotografías, instantáneas y todos los datos previamente existentes y que se encontraban en su unidad de memoria del tipo USB (Bus Serial Universal). Es de Tipo: Gratuito.

b) Riterecovery

Son tantos los dispositivos de almacenamiento con los que se trabaja hoy en día, aparte de los discos duros, que por pura estadística hay probabilidades de que los datos que contienen lleguen a dañarse, perderse o volverse corruptos.

Por esta causa siempre es práctico disponer de una herramienta como RiteRecovery. Se trata de una utilidad para recuperar datos corruptos o dañados de diskettes, discos duros, memorias ZIP, memorias USB y en general cualquier tipo de dispositivos de almacenamiento de información.

RiteRecovery trabaja con sistemas FAT12, VFAT12, FAT16, FAT32 y VFAT 12. Incluso permite recuperar de los sistemas CDFS y UDV.

c) Pc Inspector Smart Recovery

PC Inspector Smart Recovery es actualmente el único programa para recuperar datos de muchos soportes de memoria para cámaras digitales, tales como Flash Card, Smart Media, SONY Memory Stick, etc.

Sin importar si los datos, imágenes, vídeos u otros archivos fueron borrados, formateados o eliminados de forma accidental, PC Inspector Smart Recovery reconstruye de forma rápida y sencilla los ficheros.

Además, PC Inspector Smart Recovery tiene soporte para muchos formatos de imágenes, tales como JPG, TIF, CRW, entre otros, y puede recuperar archivos de vídeo en formato MOV y archivos de audio en formato WAV. Con una interfaz gráfica muy sencilla de utilizar, PC Inspector Smart

Recovery es la herramienta ideal para la recuperación de datos de tarjetas flash. Es de Tipo: Gratuito

d) Pen Drive Data Recovery

Pen Drive Data Recovery es un programa diseñado especialmente para recuperar datos perdidos o eliminados de dispositivos de almacenamiento externo como son pendrivers o tarjetas de memoria.

El programa incluso recupera datos de pen drives formateados pudiendo este ser de cualquier tamaño, 64 Mb, 128 Mb, 256 Mb, 512 Mb, 1 Gb, 2 Gb, 4 Gb, etc. Es de Tipo: Shareware.

e) Getdataback

Es potente herramienta de recuperación de archivos, capaz de recuperar los datos perdidos tras una infección de virus, un fallo general del sistema, un problema grave con el disco duro o un simple borrado accidental.

Puede recuperar los archivos de un disco duro incluso aunque Windows no lo reconozca como unidad, o se haya perdido toda la información de estructura de directorios. Es fácil de usar, gracias a su sistema de recuperación dividido en cinco pasos que te va indicando qué hacer en cada momento. GetDataBack utiliza avanzados algoritmos para garantizar la recuperación total y correcta de archivos y directorios. Es de Tipo: Shareware. El programa viene en dos versiones, una para sistemas de archivos FAT y otra para sistemas NTFS, y también permite recuperar unidades a través de red local o con un cable serie. Es de Tipo: Shareware.

f) Smart Flash Recovery

Con Smart Flash Recovery una herramienta que nos permite recuperar archivos de dispositivos extraíbles como: cámaras digitales, discos extraíbles, memoria flash USB, tarjetas de memoria Memory Stick, tarjetas PC card, tarjetas multimedia, tarjetas digitales seguras. Solo funciona en los sistemas de archivos FAT y NTFS, es muy fácil de usar, a la par que eficaz. También funciona cuando se ha perdido la tabla de particiones.

Hay que tener en cuenta, que estas herramientas también se pueden usar para recopilar datos importantes que se habían borrado de un dispositivo para que nadie los encuentre. Para estés casos les recomiendo herramientas de borrado seguro que he comentado en post anteriores. Es de Tipo: Shareware.

g) HDD Low Level Format Tool

HDD Low Level Format Tool formatea discos duros internos y externos así como memorias portátiles a través de USB y Fire-wire. Este tipo de formateo se utiliza cuando un disco se ha estropeado por diversas causas. Consiste en establecer marcas magnéticas en la superficie del disco para dividirlo en sectores que pueda reconocer el lector.

HDD Low Level Format Tool deja el disco tal y como vino de fábrica. Resulta muy recomendable tener conocimientos de hardware para saber exactamente lo que se está haciendo. No todos los formateos son iguales.

2.15.6. Cd y Dvd

a) CD/DVD Data Recovery

CD/DVD Data Recovery es una herramienta fácil de utilizar para recuperar el archivo corrompido del CD y de DVD, rápidamente explora sectores del disco, rescata los archivos dañados y copia los datos correctos al disco duro. Es de Tipo: Shareware.

b) Max Data Recovery

Software eficaz de la recuperación de los datos para el CD dañado o roto, DVD, diskettes. Es de Tipo: Gratuito.

c) DamageC opier

El programa, que puede ahorrar datos de impulsiones dañadas, CDs, DVDs, flash conduce. Es de Tipo: Gratuito.

d) Badcopy Pro

Badcopy Pro es un programa muy útil para recuperar datos de ficheros dañados de un disco duro o cualquier dispositivo de almacenamiento (disquetes, CDROM, discos ZIP, tarjetas de memorias, discos en formato UDF grabados con DirectCD e InCD, etc.)

BadCopy Pro por tanto es muy útil para: reparar disquetes dañados y recuperar sus datos, recuperar datos de discos CD-ROM, discos CD grabables (CD-R) y discos CD regrabables (CD-RW), recuperar datos de discos DVD-ROM, grabables (DVD-R) y regrabables (DVD-RW), recuperar datos inaccesibles de un disquete, disco CD, disco DVD o unidad externa flash, recuperar ficheros corruptos de disquettes, discos CD y DVD o unidades externas flash, recuperar fotos digitales de una tarjeta de memoria usada en cámaras digitales, recuperar ficheros borrados o formateados de un disquete o unidad externa USB, recuperar datos de discos Iomega Zip, Jaz, discos MO, unidades externas flash USB, etc.

Además, Badcopy Pro tiene la gran ventaja de que la recuperación no se realiza sobre el mismo soporte (no toca los archivos originales), sino sobre una carpeta que se le especifique.

e) Roadkil's Unstoppable Copier

Recuperar información de un disco (CD/DVD) que presenta daños físicos cómo ralladuras o hasta perforaciones a veces es posible gracias a un software llamado Roadkil's Unstoppable Copier en cuál puede recuperar archivos desde discos con daños físicos o con problemas cómo sectores dañados o que lanzan un error cuando tratas de leer sus datos.

El programa procurará recuperar cada pedazo legible de un fichero y poner los pedazos juntos.

Usando este método la mayoría de los tipos de ficheros pueden ser usados incluso si algunas piezas no eran recuperables en el extremo.

El programa soporta la recuperación por lotes para automatizar el uso de los programas y el trabajo de recuperar y copiar automatizado. Soporta Windows XP, Windows Vista, Windows NT, Windows 9x/Me, Windows 2000.

Más de una vez nos ha pasado que nuestra información importante almacenada en un CD o en un DVD y quizás por un rayón o golpe el m ismo nos deja de funcionar, causándonos serios problemas, generalmente la primera acción que se realiza es una limpieza con alcohol o algún liquido parecido; lo cual pocas veces llega a funcionar. Para evitar este tipo de cuestiones se tienen algunas aplicaciones de recuperación de datos que nos facilitaran la tarea, se trata de herramientas que obtienen todos esos datos que no se puedan leer desde un CD o DVD dañado.

f) CD Recovery Toolbox Free

Diseñado especialmente para CD, DVD, HD-DVD y Discos de tipo Blue-ray. Fácil de utilizar y además se ven los detalles de los archivos que contiene el medio de almacenamiento para poder recuperar datos específicos.

g) Iso Puzzle

Genera automáticamente una imagen ISO del CD completo, brinda además la posibilidad de seleccionar un sector del disco, del cual detallara los sectores defectuosos (indicados en un archivo).

h) CD Check

Recupera archivos de medios ilegibles (CD o DVD dañados). Brinda la opción de generar un hash de los archivos antes del disco para que se comparen con los actuales, en busca de algún tipo de error o modificación en el archivo.

CAPÍTULO 3. MARCO APLICATIVO

En este capítulo se realiza el análisis e implementación del proceso de Gestión de la seguridad de la información tomando como base la metodología ITIL, teniendo que cumplir ciertos procesos.

3.1. INTRODUCCIÓN

La implantación de ITIL en una empresa o entidad sea pública o privada es un proceso largo, las mejores prácticas indican que puede llegar a ser un proceso de unos 5 años, además se debe realizar de forma suave y en varias fases. La implantación de los procesos según ITIL en una empresa o entidad debe tener en cuenta los objetivos marcados por estos a medios y largos plazos. La implantación de los procesos no es una ciencia exacta ni estricta, sino que debe tener en cuenta el estado de los procesos y, de acuerdo con las mejores prácticas recogidas en los 5 publicaciones de ITIL, deben evolucionar los procesos actuales aprovechando los beneficios de la estructura actual y mejorando o implantando los procesos cuyas deficiencias obstaculizan la evolución de la entidad y la alineación de la tecnología y el negocio.

Dentro el conjunto de procesos a implementar dentro la metodología ITIL, tenemos que tomar en cuenta las consideraciones que son base para realizar la demostración de la hipótesis planteada, partiendo de un análisis que involucre las normas mencionadas en anteriores apartados.

3.2. ESTUDIO DE LA SITUACIÓN ACTUAL DE LAS ORGANIZACIONES.

En nuestro país Bolivia el tema de Seguridad informática se encuentra aún en proceso de implementación aunque en los últimos años se ha avanzado mucho. Parte de la responsabilidad de que esto ocurra, recae sobre nuestras universidades, que ofrecen formación mínima en el área, una o dos materias dentro de la malla curricular de las carreras de ingeniería de sistemas e Informática. Las universidades no tienen toda la culpa, también los gerentes y dueños de empresas tienen su responsabilidad de que esto suceda, debido a que casi nunca facilitan los recursos necesarios requeridos al departamento de sistemas para una administración segura y eficiente y mucho menos para capacitar y concientizar en materia de seguridad a su personal.

Nuestro país no se cuenta con un estudio en el que se analice el impacto de las TIC y la Seguridad Informática dentro las entidades públicas o privadas y esto es esencialmente por la falta de reglamentos que describan buenas prácticas que nos den un panorama de las normativas existentes en cada organización o entidad enfocados a la realidad de nuestras organizaciones.

Por todo esto tomaremos en cuenta otros estudios realizados a nivel latino americano en especial el estudio realizado por la CEPAL sobre Seguridad Informática, según este estudio estima que el 43% de las empresas reconoció haber tenido algún incidente en sus sistemas, lo que llevó a que el 63% de las consultadas señalara que preveía una mayor inversión en la seguridad de sus sistemas de computación y almacenamiento de datos.

TIPOS DE ATAQUES	2009	2008	2007	2006
Virus	75	80	85	90
Abuso de internet	55	78	75	85
Robo de portátiles/móviles	50	60	55	70
Acceso no autorizado a la información	40	45	40	55
Penetración del sistema	38	40	38	35
Negación del servicio	18	30	28	35
Robo de información propietaria	9	18	16	25
Sabotaje	5	20	5	18
Fraude financiero	5	18	20	20

Tabla 1: Tipos de ataques en Sistemas informaticos.
Fuente: CSI/FBI Computer Crime and Security Survey.

Este dato se refería solamente a las entidades privadas, pero indica claramente que sin recursos es muy difícil oponerse a estos tipos de crímenes, aun en presencia de normas específicas internas.

Además, este estudio indica que los departamentos de informática o de seguridad TI, se encuentran centralizadas, esto quiere decir que podemos implementar con más facilidad los procesos ITIL.

Este estudio cree que la forma adecuada de avanzar es con el uso de las TIC para cambiar los procesos de gestión de las entidades. Esto es un punto fuerte de cara al proyecto de implantación de ITIL en entidades u organizaciones, ya que supone un apoyo al proyecto de la dirección de la entidad, algo fundamental en un proyecto de

estas características, el cual requiere inversión económica y cambios sustanciales en la organización y la forma de trabajar de las organizaciones.

3.2.1. Problemas Internos Detectados Dentro las Entidades.

A raíz de los estudios realizados sobre el funcionamiento interno actual dentro de las entidades tanto públicas como privadas a nivel de seguridad de la información, se ha detectado diversos problemas

- Virus
- Abuso de Internet
- Acceso no autorizado a la información
- Negación del servicio
- Robo de información propietaria
- Sabotaje y ataques internos por el personal.

Por otro lado las entidades tienen ciertas características que pueden influir negativamente en la implantación de los procesos ITIL, pero que sin embargo, conociéndolos de antemano son puntos clave en los que focalizarse durante la implantación de ITIL.

En un entorno informático existen una serie de recursos (humanos, técnicos, de infraestructura) que están expuestos a diferentes tipos de riesgos en este caso se hablara de los riesgos que corren la información de las entidades u organizaciones, tratar de minimizar los efectos del problema de seguridad se realiza lo que se denomina un análisis de riesgo, una vez que se conocen los recursos en este caso la información que se debe proteger, es la hora de identificar las vulnerabilidades y amenazas que conciernen contra la información

La clasificación e riegos a estudia y medias de protección, suele realizarse en base al nivel de importancia del daño causado y a la probabilidad aproximada de que es daño se convierta en realidad.

Evidentemente, los recursos que presentan un riesgo evaluado, mayor serna las medidas de protección que deben poseer, ya que esto significa que es probable que sean atacados, y que además el ataque puede causar pérdidas importantes. En caso de que ocurra aun sabiendo los riegos se proseguirá a protegerlos.

RIESGOS	CAUSAS	IMPACTO	NIVEL DE RIESGO
Virus en equipos de computo	Antivirus caducado, escaneo no frecuente.	Como consecuencia los equipos se infectan de virus que circulan a través de la red y circulan por la red modificando o eliminado los la información dentro de esta.	**Controlable**
Falta de no-break en equipos y servidores	Falta de los recursos materiales por parte de la gerencia	Provoca que los equipos tengan daños en los dispositivos dentro de este, perdiendo la información	**Potencial**
Penetración de intrusos a la información	Dar claves de recursos materiales por parte del personal	Perdida de datos y modificación de estos.	**Controlable**

Modificación de la información por personas no autorizadas	Falta de una cultura informática	Perdida de la información real	**Potencial**
Robo de la información por parte de los usuarios	Falta de un control de la administración de la TI.	Perdida de la información y dinero	**Controlable**
Falla de los discos de los servidores	Tiempo de vida agotada de los dispositivos en los servidores	Los datos son en muchos casos inservibles esto ocasiona pérdida de tiempo y recuperación y dinero	**Controlable**
Corrupción de los datos	Constantes transacciones en las actividades, fallos en los UPS y falta de monitoreo en los servidores	No hay credibilidad en los usuarios que manejan los datos	**Controlable**
Perdida de la información	Falta de respaldo constante de los servidores	Los empleados pierden tiempo en la captura	**Controlable**
Riesgos en los equipos de computo	Falta de contraseñas en los equipos	La gente externa y usuarios extraigan la información y la modifiquen	**Controlable**

Falta de clasificación en responsabilidades	Falta de organización y tiempo	Los usuarios hacen lo que quieren y no entregan bien sus trabajos.	**Controlable**
Vulnerabilidad en la red contra la penetración de intrusiones	Falta de un IPS	Esto con lleva a la penetración de intrusos y daño a la red.	**Controlable**
Falta de conocimiento del usuario	Falta de capacitación hacia los usuarios	Malos resultados antes y después de un desastre.	**Controlable**
Errores en las aplicaciones	Fallo por errores de programación y por falta de capacitación a quienes la instalan	Perjudica a la empresa en la perdida de información y mal uso de esta.	**Potencial**
Fallas en las comunicaciones de la red interna	Caídas temporales de esta por falta de suministro eléctrico, problemas en el cableado	Problemas en la seguridad y cortes en la comunicación y la imposibilidad de comunicar a la empresa con el exterior	**Controlable**
No existe una política de contraseñas para el acceso a los equipos	Falta de un plan de concientización hacia los usuarios	Robo de información de los mismos usuarios y haciendo uso indebido de esta.	**Potencial**

Tabla 2: Riesgos, causas e impactos que se encuentran en las entidades
Fuente: Elaboración propia.

Por ello las entidades u organizaciones requieren de un estándar que cuente con las siguientes funcionalidades:

- Alta disponibilidad, en caso de que exista alguna contingencia en la infraestructura de las entidades, el servicio debe de ser continuo, siempre y cuando esta contingencia afecte a una de las conexiones con las que cuenta.
- Balanceo de cargas, siempre que toda la infraestructura esté funcionando, las entidades u organizaciones requieren tener al máximo, lo que se requiere para lo cual se necesita que los usuarios sean distribuidos equitativamente que la infraestructura con la que cuentan.
- Tecnologías heterogéneas, los estándares de seguridad indican que se requiere más de una tecnología para no comprometer ningún servicio externo de la organización, es por esto que se tomó la decisión de implementar un estándar basado en ITIL que cubra estas necesidades.
- Clasificación de las necesidades de los usuarios.

3.3. CLASIFICACIÓN DE LAS ÁREAS DE RIESGOS.

Se clasifican las áreas ya que es de suma importancia saber cuáles de estas son las que tienen prioridad para mantener una mejor protección hacia sus datos.

Los ordenaremos de bajo, mediano y alto riesgo.

3.3.1. Áreas de Bajo Riesgo.

- Almacén e inventarios
- Recursos materiales
- Normas
- Dirección de planeación y vialidad
- Dirección de evaluación e infraestructura

3.3.2. Áreas de Mediano Riesgo.

- Información publica
- Dirección operativa
- Recursos Humanos

3.3.3. Áreas de Alto Riesgo.

- Recursos financieros
- Dirección jurídica
- Dirección informática
- Contraloría interna

3.4. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Los principales objetivos de la Gestión de la Seguridad se resumen en:

- Diseñar una política de seguridad, en colaboración con clientes y proveedores, correctamente alineada con las necesidades del negocio.
- Asegurar el cumplimiento de los estándares de seguridad acordados en los SLAs.
- Minimizar los riesgos de seguridad que amenacen la continuidad del servicio.

La correcta Gestión de la Seguridad no es responsabilidad exclusiva de expertos en seguridad que desconocen los otros procesos de negocio. Si caemos en la tentación de establecer la seguridad como una prioridad en sí misma, limitaremos las oportunidades de negocio que nos ofrece el flujo de información entre los diferentes agentes implicados y la apertura de nuevas redes y canales de comunicación.

La Gestión de la Seguridad debe conocer en profundidad el negocio y los servicios que presta la organización TI para establecer protocolos de seguridad que aseguren

que la información esté accesible cuando es necesaria para aquellos que tengan autorización para utilizarla.

Una vez comprendidos cuáles son los requisitos de seguridad del negocio, la Gestión de la Seguridad debe supervisar que estos se hallen convenientemente plasmados en los SLAs correspondientes para, a renglón seguido, garantizar su cumplimiento.

La Gestión de la Seguridad debe asimismo tener en cuenta los riesgos generales a los que está expuesta la infraestructura TI, y que no necesariamente tienen por qué figurar en un SLA, para asegurar, en la medida de lo posible, que no representan un peligro para la continuidad del servicio.

Es importante que la Gestión de la Seguridad sea proactiva y evalúe a priori los riesgos de seguridad que pueden suponer los cambios realizados en la infraestructura, nuevas líneas de negocio, etcétera.

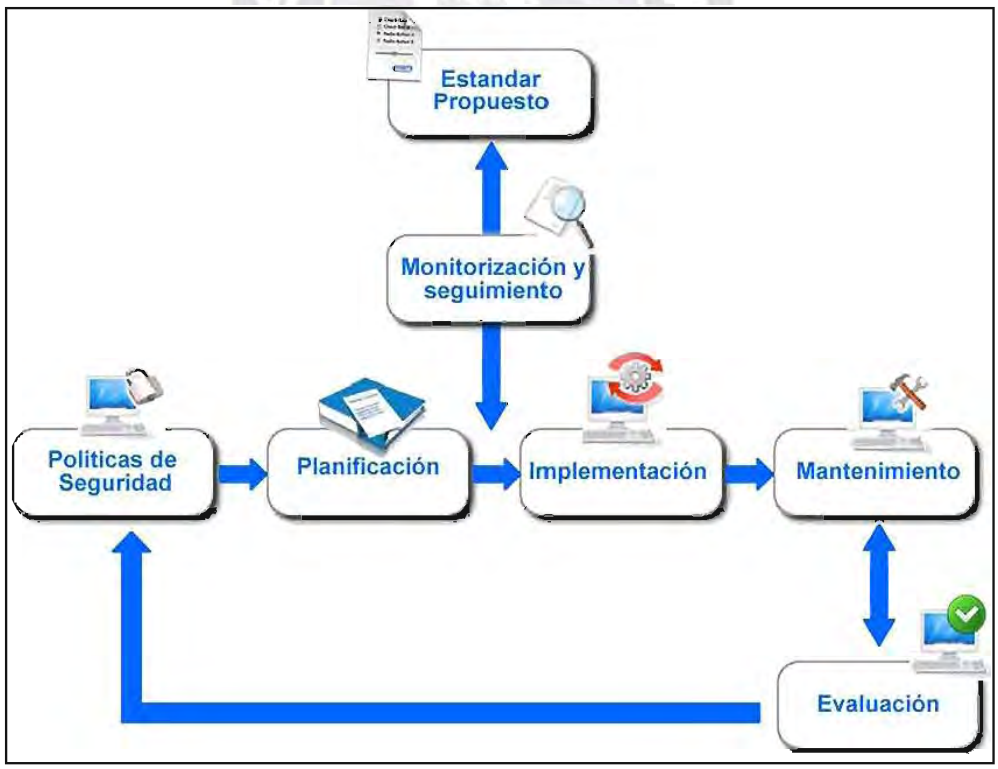


Figura 9: Interacción del estándar propuesto y las funciones de la Gestión de la Seguridad. Fuente: Elaboración propia.

3.5. PROCESOS DE LA GESTION DE LA SEGURIDAD DE LA INFORMACION.

La Gestión de la Seguridad está estrechamente relacionada con prácticamente todos los otros procesos TI de la metodología ITIL y necesita para su éxito la colaboración de toda la organización.

Para que esa colaboración sea eficaz, es necesario que la Gestión de la Seguridad:

a) Establezca una clara y definida política de seguridad que sirva de guía a todos los otros procesos.

b) Elabore un Plan de Seguridad que incluya los niveles de seguridad adecuados tanto en los servicios prestados a los clientes como en los acuerdos de servicio firmados con proveedores internos y externos.

- Implemente el Plan de Seguridad.
- Monitorice y evalúe el cumplimiento de dicho plan.
- Supervise proactivamente los niveles de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades.
- Realice periódicamente auditorías de seguridad.

3.5.1. Proceso Política y Plan de Seguridad.

Es imprescindible disponer de un marco general en el que encuadrar todos los subprocesos asociados a la Gestión de la Seguridad. Su complejidad e intricadas interrelaciones necesitan de una política global clara en donde se fijen aspectos tales como los objetivos, responsabilidades y recursos.

En particular la Política de Seguridad debe determinar:

- La relación con la política general del negocio.
- La coordinación con los otros procesos TI.

- Los protocolos de acceso a la información.
- Los procedimientos de análisis de riesgos.
- Los programas de formación.
- El nivel de monitorización de la seguridad.
- Qué informes deben ser emitidos periódicamente.
- El alcance del Plan de Seguridad.
- La estructura y responsables del proceso de Gestión de la Seguridad.
- Los procesos y procedimientos empleados.
- Los responsables de cada subproceso.
- Los auditores externos e internos de seguridad.
- Los recursos necesarios: software, hardware y personal.

El objetivo del Plan de Seguridad es fijar los niveles de seguridad que han de ser incluidos como parte de los SLAs, OLAs y UCs.

Este plan ha de ser desarrollado en colaboración con la Gestión del Nivel de Servicio, que es la responsable en última instancia tanto de la calidad del servicio prestado a los clientes como la del servicio recibido por la propia organización TI y los proveedores externos.

El Plan de Seguridad debe ser diseñado con el fin de ofrecer un mejor y más seguro servicio al cliente y nunca como un obstáculo para el desarrollo de sus actividades de negocio.

Siempre que sea posible, deben definirse métricas e indicadores clave que permitan evaluar los niveles de seguridad acordados.

Un aspecto esencial a tener en cuenta es el establecimiento de unos protocolos de seguridad coherentes en todas las fases del servicio y para todos los estamentos implicados. "Una cadena es tan resistente como el más débil de sus eslabones", por lo que carece de sentido, por ejemplo, establecer una estrictas normas de acceso si una aplicación tiene vulnerabilidades frente a inyecciones de SQL. Quizá con ello podamos engañar a algún cliente durante algún tiempo ofreciendo la imagen de "fortaleza", pero esto valdrá de poco si alguien descubre que la "puerta de atrás está abierta".

3.5.2. Aplicación de las Medidas de Seguridad.

Por muy buena que sea la planificación de la seguridad resultará inútil si las medidas previstas no se ponen en práctica.

Es responsabilidad de la Gestión de Seguridad coordinar la implementación de los protocolos y medidas de seguridad establecidas en la Política y el Plan de Seguridad.

En primer lugar la Gestión de la Seguridad debe verificar que:

- El personal conoce y acepta las medidas de seguridad establecidas así como sus responsabilidades al respecto.
- Los empleados firmen los acuerdos de confidencialidad correspondientes a su cargo y responsabilidad.
- Se imparte la formación pertinente.

Es también responsabilidad directa de la Gestión de la Seguridad:

- Asignar los recursos necesarios.
- Generar la documentación de referencia necesaria.
- Colaborar con el Centro de Servicios y la Gestión de Incidentes en el tratamiento y resolución de incidentes relacionados con la seguridad.

- Instalar y mantener las herramientas de hardware y software necesarias para garantizar la seguridad.
- Colaborar con la Gestión de Cambios y la de Entregas y Despliegues para asegurar que no se introducen nuevas vulnerabilidades en los sistemas en producción o entornos de pruebas.
- Proponer RFCs a la Gestión de Cambios que aumenten los niveles de seguridad.
- Colaborar con la Gestión de la Continuidad del Servicio para asegurar que no peligra la integridad y confidencialidad de los datos en caso de desastre.
- Establecer las políticas y protocolos de acceso a la información.
- Monitorizar las redes y servicios en red para detectar intrusiones y ataques.

Es necesario que la gestión de la empresa reconozca la autoridad de la Gestión de la Seguridad respecto a todas estas cuestiones y que incluso permita que ésta proponga medidas disciplinarias vinculantes cuando los empleados u otro personal relacionado con la seguridad de los servicios incumplan con sus responsabilidades.

3.5.3. Evaluación y mantenimiento.

a) Evaluación.

No es posible mejorar aquello que no se conoce, por lo que resulta indispensable evaluar el cumplimiento de las medidas de seguridad, sus resultados y el cumplimiento de los SLAs.

Aunque no es imprescindible, es recomendable que estas evaluaciones se complementen con auditorías de seguridad externas y/o internas realizadas por personal independiente de la Gestión de la Seguridad.

Estas evaluaciones/auditorias deben valorar el rendimiento del proceso y proponer mejoras que se plasmarán en RFCs que habrán de ser evaluados por la Gestión de Cambios.

Independientemente de estas evaluaciones de carácter periódico, se deberán generar informes específicos cada vez que ocurra algún incidente grave relacionado con la seguridad. De nuevo, si la Gestión de la Seguridad lo considera oportuno, estos informes se acompañaran de las RFCs correspondientes.

b) Mantenimiento.

La Gestión de la Seguridad es un proceso continuo y se han de mantener al día el Plan de Seguridad y las secciones de seguridad de los SLAs.

Los cambios en el Plan de Seguridad y los SLAs pueden ser resultados de la evaluación arriba citada o de cambios implementados en la infraestructura o servicios TI.

No hay nada más peligroso que la falsa sensación de seguridad que ofrecen medidas de seguridad obsoletas.

Es asimismo importante que la Gestión de la Seguridad esté al día en lo que respecta a nuevos riesgos y vulnerabilidades frente a virus, spyware, ataques de denegación de servicio, etcétera, y que adopte las medidas necesarias de actualización de equipos de hardware y software, sin olvidar el apartado de formación: el factor humano es normalmente el eslabón más débil de la cadena.

3.6. CONTROL DEL PROCESO.

Al igual que en el resto de procesos TI, es necesario realizar un riguroso control del proceso para asegurar que la Gestión de la Seguridad cumple sus objetivos.

Una buena Gestión de la Seguridad debe traducirse en:

- Disminución del número de incidentes relacionados con la seguridad.

- Un acceso eficiente a la información por el personal autorizado.
- Gestión proactiva, que permita identificar vulnerabilidades potenciales antes de que estas se manifiesten y provoquen una seria degradación de la calidad del servicio.

La correcta elaboración de informes permite evaluar el rendimiento de la Gestión de Seguridad y aporta información de vital importancia a otras áreas de la infraestructura TI.

Entre la documentación generada cabría destacar:

- Informes sobre el cumplimiento, en lo todo lo referente al apartado de seguridad, de los SLAs, OLAs y UCs en vigor.
- Relación de incidentes relacionados con la seguridad, calificados por su impacto sobre la calidad del servicio.
- Evaluación de los programas de formación impartidos y sus resultados.
- Identificación de nuevos peligros y vulnerabilidades a las que se enfrenta la infraestructura TI.
- Auditorías de seguridad.
- Informes sobre el grado de implementación y cumplimiento de los planes de seguridad establecidos.

3.7. PROPUESTA ESTÁNDAR PARA PARA IMPLEMENTACION DE LA METDOLOGIA ITIL V3.

De esta manera proponemos el estándar de seguridad de la información para todo entidad, con el cual tendrá un mejor plan para resguardar la información y en caso de ocurrir un desastre contar con un plan de contingencia para la recuperación de la información. Así se pretende prevenir los errores anteriormente mencionados en la problemática que ocurre dentro las entidades.

Se ofrece una propuesta adecuada que contempla todos los aspectos mencionados en los capítulos anteriores se hizo un estudio detallado del y módulos correspondientes, las aplicaciones con las que trabajaban y los tiempos de respuesta obtenidos, observando que la respuesta del sistema es lenta y considerando a futuro la actualización tecnológica para estar a la vanguardia de comunicaciones y poder brindar un mejor servicio para los usuarios así como clientes.

Se contempla el hacer uso de conciencia por parte de los usuarios, aligerando los riesgos que pueden ocurrir debido a la falta de capacitación hacia ellos.

3.7.1. Estructura del estándar

En base a la situación actual dentro las entidades, las normas, estándares, métodos, herramientas de protección y de recuperación existentes, se crea un estándar en el cumplimiento de la protección y recuperación de datos. El cual consta de las siguientes partes:

a) Política de Protección a los datos.

- Protección en la organización
- Infraestructura de la protección de los datos
- Acceso externo e interno

b) Clasificación y control de activos.

- Clasificación de los activos
- Clasificación de los datos
- Responsabilidad de acceso

c) Responsabilidad del personal.

- Responsabilidades en la protección de la información

- Capacitación al usuario

d) Seguridad física y del entorno.

- Áreas protegidas
- Seguridad del equipo de computo

e) Comunicaciones.

- Control de acceso a la red
- Control de acceso a las aplicaciones en red
- Protección para intrusiones
- Acceso al sistema de monitoreo y su uso
- Acceso vía VPN
- Acceso a Internet

f) Administración Informática.

- Administración en redes
- Administración de los equipos de computo

g) Recuperación ante desastres.

- Políticas de la recuperación de datos
- Organización y clasificación de los datos
- Alternativas de recuperación

Se crea un modelo de protección y recuperación de datos que se muestra a continuación.

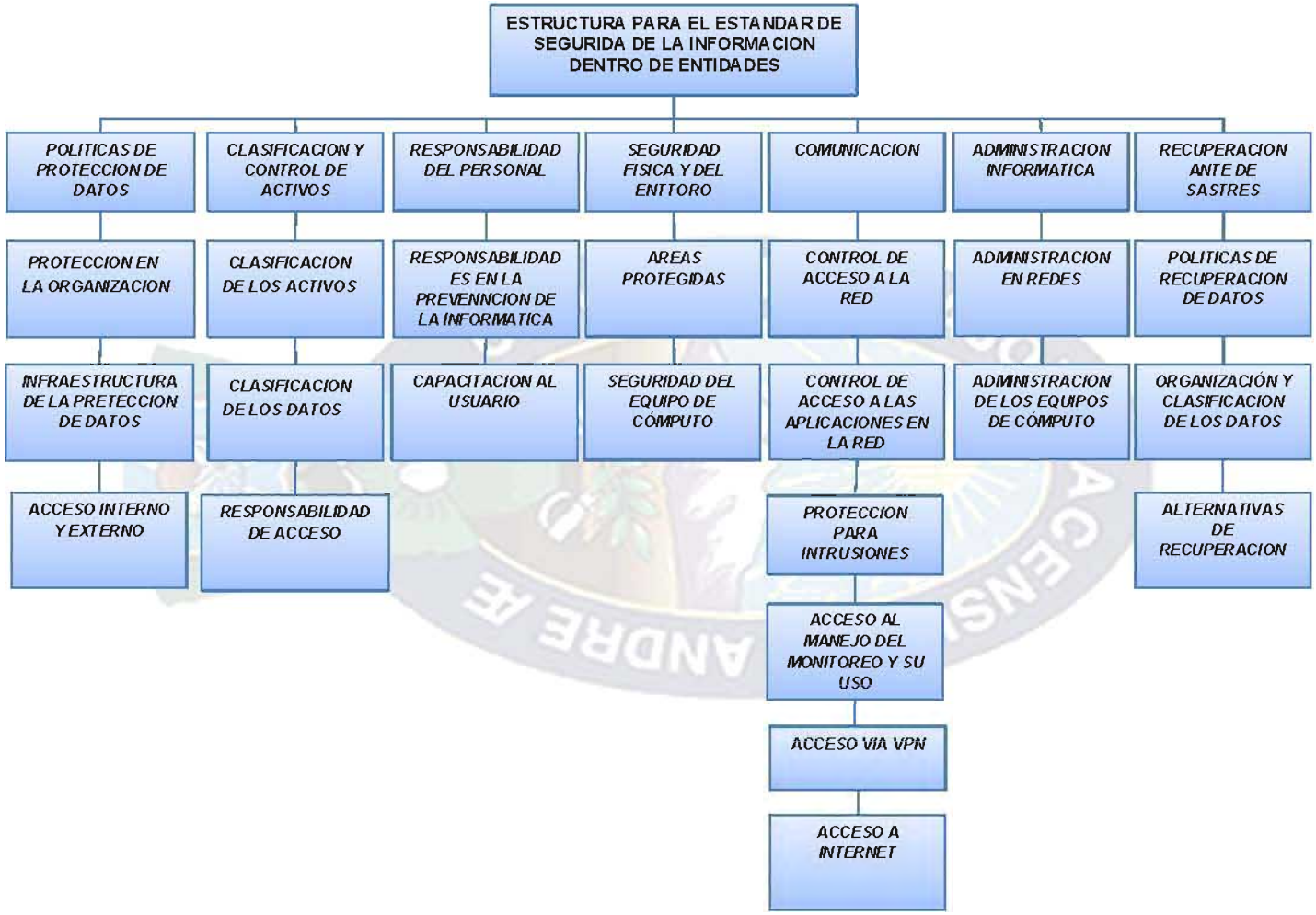


Grafico 2: Modelo de protección y recuperación de datos que se genera para una Entidad
Fuente: Elaboración Propia

3.7.2. Política de Protección a los datos.

Las políticas de protección que se visualizan en dentro las entidades para prevenir el robo, modificación y pérdida de la información, están las normas que se requieren para su buen funcionamiento garantizando la continuidad, disminuyendo riesgos y que los objetivos sean cumplidos, es importante que al aplicar las políticas se tenga en cuenta los siguientes aspectos:

- Informar a los usuarios sobre el desarrollo de las políticas, riesgos y ventajas de estas.
- Definir clasificación de responsabilidades por cada área.
- Monitorear continuamente los procedimientos y operaciones de la entidad de forma tal, que ante cambios las políticas puedan actualizarse oportunamente para prevenir los riesgos.
- Especificar concretamente el alcance de las políticas con el fin de respondan conforme al objetivo planteado.

La cual está dividida en los siguientes cinco puntos.

a) Protección en la organización.

Una entidad requiere mantener sus actividades operativas en secreto, las cuales resguarda celosamente por lo que se tomara en cuenta las siguientes medidas:

- Mantener la seguridad tanto para el personal restringiendo el acceso a los externos, así mismo otorgar el permiso adecuado a su personal, ya que una falla en esto, puede ocasionar el mal uso de la información que la empresa tiene.
- Mantener los permisos del personal actualizados, ya que de no hacerlo puede provocar que el personal que laboró de manera activa, llegue a

generar un descontrol y provocar pérdidas de los secretos operativos de la empresa en cuestión.

b) Infraestructura de la protección de los datos.

La infraestructura de la entidad es parte vital de la misma, ya que en esta se realizan las actividades diarias, por lo cual se deben de tomar las siguientes medidas para prevenir cualquier pérdida de información y asegurar que esté protegida, ya que tiene un mínimo control central políticas y estándares inexistentes, todo esto con la finalidad de otorgar los permisos de acceso locales y remotos a recursos de red y aplicaciones críticas de negocio, brindando un mayor soporte y control.

Para equipos de cómputo:

- Uso de un usuario y un password, el cual debe ser de una longitud mínima de 8 caracteres el cual debe de cambiar por lo menos cada mes, esto con el fin de mantener la seguridad en el acceso a los equipos de cómputo.
- Los passwords deben ser únicos y no se deben de repetir por lo menos con 5 meses de anterioridad, deben de incluir por lo menos un carácter en mayúsculas, minúsculas, números y algún carácter especial.
- Los usuarios y passwords son de carácter personal, por lo cual no se deben de prestar

Para el acceso:

- Todos los empleados deberán traer visible su identificación que los acredite como tal durante su estancia en la organización.
- Los visitantes, son todos los que no son empleados, deberán portar su gafete de visitante durante su estancia en las instalaciones.

- El usuario deberá respetar y cuidar de las instalaciones, reportando el daño de la misma, en caso de existir, al personal encargado del mantenimiento de este.

c) Acceso externo e interno.

El acceso externo a la entidad u organización será controlado otorgando una identificación que indique el estatus de visitante y sea distinta a las usadas por el personal interno para tener un mejor control del acceso evitando perdidas y personal no autorizado.

- El acceso de los empleados vía remota a la red de la organización, esta debe ser mediante el uso de una conexión segura implementada mediante una VPN, formulando políticas en donde la persona que manejara los programas tenga password y contraseña para el acceso.
- Los visitantes deben de registrarse en la recepción dejando una identificación oficial y otorgarles la credencial de acceso externo.
- Los trabajadores, deben de presentar su credencial que los acredite como tal, durante su estancia en la organización.
- El empleado está obligado a reportar cualquier anomalía en el uso del gafete.
- El empelado no deberá de prestar su gafete ya que este es personal.

3.7.3. Clasificación y control de activos.

La clasificación de los activos en la entidad estudiada es el indicador de los niveles de protección y acceso que se deben de implementar ya que estos mientras más importantes sean más cuidado se deben de tener hacia ellos.

Es por esto que se deben de diferenciar los tipos de activos que se desean proteger y se nombrara algún tratamiento especial conforme a su clasificación según los siguientes puntos.

a) **Clasificación de los activos.**

Es la información más importante tanto para la entidad como para los usuarios. Estos se clasifican en:

- Computadoras de escritorio
- Computadoras portátiles móviles
- Servidores
- Routers
- Dispositivos de memoria
- Discos duros extraíbles

b) **Clasificación de los datos.**

La finalidad de la clasificación de los datos en la entidad es identificar cual son las más importante para poder resguardarla en caso de algún desastre.

La clasificación de los datos es la siguiente:

- Datos confidenciales: Son aquellos datos que afectan directamente a las decisiones de la entidad así como los datos de carácter personal que se han definido con anterioridad.
- Datos privados: Son los datos a los que solo los empleados pueden acceder, por lo que se consideran pertenecientes a la entidad.
- Datos públicos: Son aquellos con los que la organización publica sus promociones y ofertas en el mercado.

Los datos de los usuarios ellos serán los encargados de clasificarlos dependiendo del grado critico además de mantenerla actualizada.

c) Responsabilidad de acceso.

La responsabilidad de acceso recae principalmente al usuario de la entidad sin embargo se crearon las siguientes políticas para hacer conciencia sobre ellos de estos datos, ya que es algo que no toman en cuenta.

El acceso a estos también recae en el área de informática ya que actualmente, la mayor parte de los datos es transmitida mediante correos electrónicos o se genera en equipos de cómputo.

Las políticas a cumplir son:

- Establecer el nivel de acceso físico según el rol del empleado
- Establecer un nivel de acceso de datos en la red según lo requerido por cada rol de usuario.
- Limitar los equipos de los usuarios mediante las políticas que se generen en el sistema operativo, restringiendo el acceso a dispositivos externos, lectores ópticos y utilizando una contraseña.
- Limitar el acceso a los recursos de red que no se requieran, así como el acceso a la Internet.

3.7.4. Responsabilidades del personal.

La responsabilidad es el punto fuerte de la seguridad de toda entidad ya que nos concientiza de las acciones que se realizan día a día. Para evitar estos descuidos ante riesgos que ocurren en la entidad continuamente si no se tienen procedimientos para salvaguardar la información hay perdida.

Dentro de la responsabilidad del usuario se encuentran los siguientes puntos:

- Mantener en secreto sus passwords de cada uno de los sistemas
- Reportar las anomalías del sistema.

- Cambiar sus passwords cada mes mínimo.
- Asistir a los cursos impartidos por las dirección informática
- Aprobar las evaluaciones de los cursos que se impartan
- Solicitar los programas y permisos para realizar su trabajo, explicando el porqué de los mismos.
- Comprometerse con los lineamientos de la institución
- Mantener en secreto la metodología empleada para la protección de los equipos de cómputo y la infraestructura de la misma.
- Cuidar de los equipos con los recursos de la empresa.

Por lo tanto es importante la prevención de problemas dentro de la entidad, también el más difícil de generar ya que esto es con base al compromiso del empleado y dependerá de la entidad para implementar estas políticas y capacitar al usuario en ellas.

d) Responsabilidades en la protección de la información.

La responsabilidad de la protección de la información de la entidad, recae en todo el personal de la empresa, dedicando un esfuerzo en hacer llegar las políticas a todo el personal de esta, ya que en ellos recae la fortaleza de estas medidas.

Las áreas directivas en conjunto con la dirección de informática y Recursos Humanos deben impartir cursos que concienticen la importancia de estas políticas.

Así mismo el área de informática de la entidad debe de generar cursos para la concientización de la seguridad y dar a conocer los principales riesgos latentes.

e) Capacitación al usuario.

La capacitación de los empleados, debe ser constante y simple, de forma que se pueda comprender, por lo que se sugiere que cumpla con las siguientes características:

- La capacitación debe de ser creativa y comprensible para cualquier miembro de la entidad, ya que de no ser así, esta no cubrirá su objetivo.
- Debe de existir alguna evaluación a los capacitados para comprobar que este último comprenda lo mínimo que se desea impartir.
- También debe de dar solución a las inquietudes de los empleados sin dar a conocer los detalles de cómo se está protegiendo la institución.

3.7.5. Seguridad física y del entorno.

Se trata sobre la seguridad física de los sistemas informáticos de la entidad (ordenadores, hardware de red, dispositivos electrónicos, etc.), de todo el entorno que los rodea en el lugar donde se hallan ubicados (edificio, sistemas eléctricos, seguridad de las cerraduras, sistemas de supresión de incendios) y de las personas que están encargadas de su vigilancia o de la vigilancia del acceso a estos sistemas informáticos (administradores, personal externo, vigilantes, etc.).

En cuanto al acceso a las instalaciones debe de ser controlado por el personal de seguridad contratado, así mismo se debe de implementar algún método de acceso a las instalaciones, el cual es gestionado por el área de seguridad general, teniendo como opciones desde el colocar a un supervisor en el acceso hasta la implementación de lectores de tarjetas para el acceso.

a) Áreas protegidas.

Son aquellas áreas importantes para la entidad en donde se mantenga la información como el SITE o sitio de internet que es uno de las principales, este debe estar acondicionado y estar bajo llave donde solamente las deben de tener

el personal indicado y debe existir un letrero indicando que solo el personal autorizado puede acceder.

Estas áreas básicamente en toda empresa son:

- Bodegas de materias primas
- Bodegas de producto terminado
- Cuarto de servidores o Site principal

Otras áreas restringidas son la de producción y la de informática sin embargo esta no puede estar bajo llave ya que el flujo del personal es mayor sin embargo el acceso de los externos debe de ser supervisado y monitoreado permanentemente por seguridad y por el empleado al que se visita.

b) Seguridad del equipo de cómputo

La seguridad de los equipos personales es principalmente responsabilidad de los usuarios, sin embargo el área de informática debe de publicar las normas a las cuales está sujeto el empleado además de contratar un personal de vigilancia para monitorear el acceso de entrada y salida de los equipos.

Entre estas normas se encuentran:

- El empleado que lo requiera deberá contar con un equipo personal
- El empleado deberá de contar con un usuario y un password siempre y cuando cuente con un equipo de computo
- El equipo debe permanecer bloqueado cuando el usuario se desplace de su ubicación, así mismo debe de apagarlo al finalizar su horario laboral.
- Indicar al personal de soporte técnico la instalación de programas y configuración adecuada el puesto en caso de no contar con ella.

- El equipo deberá estar conectado a un no-break para evitar descargas eléctricas.

3.7.6. Comunicaciones.

Las comunicaciones son la base hoy en día de toda entidad, ya que en ella se basa la transferencia de la información de las direcciones a gerencias con sus clientes u empleados.

Además se usaran medidas y controles para denegar el acceso a través de las redes a personas no autorizadas, así como para garantizar la legitimidad de las partes en comunicación.

La seguridad de las comunicaciones incluye transmisiones, emisiones y seguridad física

a) Control de acceso a la red

Reducir el riesgo y los costos de la seguridad en la entidad u organización, identificando e impidiendo las amenazas y vulnerabilidades, por medio de una evaluación constante de todos los equipos con respecto a las políticas definidas, el control de acceso a la red puede verificar que estén actualizados, que los parches de seguridad están instalados y que no se utilizan aplicaciones no permitidas, los usuarios accedan solamente a lo requiera su trabajo, que el ancho de banda no sea consumido y los usuarios que se enlazan vía VPN infecten o saboteen la información.

La red debe de ser controlada en base a la política adecuada para cada empresa, sin embargo los puntos generales a tomar en cuenta en las entidades son:

- Restringir el acceso a la red por parte de cualquier dispositivo que pueda tener acceso a esta, ya sea mediante los nodos establecidos o por la red inalámbrica en caso de existir.
- Limitar el acceso del usuario únicamente a la entidad.

- a los recursos que requiere para desarrollar su trabajo.
- Los nodos que existan en las salas de juntas o áreas a las que se pueda tener acceso con facilidad deberán estar deshabilitadas mientras no se requiera de su uso por parte de la empresa; así mismo se debe de contar con un calendario para conocer los días de uso de estas áreas.
- La red inalámbrica debe de contar con una contraseña y no debe de funcionar con administrador de IP en el router.
- La red en general debe de contar con IP fija para cada uno de los equipos de la organización, distribuyendo los rangos ya sea por área o por ubicación física para una mejor administración.
- Debe de tenerse un control del acceso a los datos de la red restringiendo los permisos de acceso a archivos en las carpetas de los servidores de documentos con el fin de mantener un control sobre el acceso a estos.
- El acceso a Internet debe ser autorizado por el jefe inmediato del usuario y su jefe de área así como tener el visto bueno del jefe del área de redes.
- La red debe de contar con un sistema de seguridad el cual debe constar como mínimo por un firewall, un IDS y un Sniffer el cual debe de estar en modo promiscuo.
- Los derechos de acceso de usuarios deben ser revisados periódicamente.
- Limitar los lugares desde donde el usuario puede conectarse.

b) Control de acceso a las aplicaciones en red.

El acceso a las aplicaciones en la red de la entidad deriva de dos partes, las de la intranet y las del Internet.

En la intranet se encuentran varias aplicaciones tales como el acceso a las bases de datos, el portal corporativo o alguna aplicación web generada para la información y la operación de los empleados.

Las aplicaciones de Internet generadas por la entidad son las que se utilizan tanto para dar información de esta como para el servicio a los clientes. Estos deben de estar dentro de las siguientes normas:

Tener usuario y password para las aplicaciones. El password debe de ser de 8 caracteres como mínimo, dentro de los cuales debe de por lo menos existir un carácter en mayúsculas, en minúsculas, números y caracteres especiales, exceptuando los mencionados a continuación:

- Igual que. Menor que, corchetes, comillas simples y comillas dobles, menor y mayor que.
- Las aplicaciones web como portales de transacciones y webservices deben de contar con certificados de seguridad y los usuarios y passwords deben de estar encriptados.
- Los certificados de las aplicaciones deben de renovarse periódicamente siempre y cuando sea trate de una dependencia de la organización.

c) Protección para intrusiones

Ante las amenazas que existen en el interior y exterior de las entidades para la destrucción de datos y acceso a ellos se requiere de una protección para buscar ataques de hackers permitiendo que los usuarios reaccionen frente a violaciones de seguridad antes de que ocurra algún peligro en la red y en los equipos de cómputo. Para esto es recomendable hacer políticas flexibles de lo que se desea bloquear para control total de todos los métodos de detección de ataques para adaptarse a las aplicaciones de protección más exigentes. Para el tipo de información que se maneja en las entidades se recomienda usar un IPS ya q analiza y bloque el paso de los intrusos.

d) Acceso al sistema de monitoreo y su uso

Es importante que las entidades cuente con este método para saber cómo está funcionando el acceso interno y externo con el fin de prevenir riesgos.

El sistema de monitoreo será incorporado mínimo por un firewall, un IPS y un Sniffer, para un buen funcionamiento, el acceso a estos es exclusivo del personal encargado de la red.

El monitoreo debe de ser diario para la revisión de los logs generados y se creara una base de conocimientos con forme a los resultados de estos logs, entradas o bloqueos de gente no autorizada.

e) Acceso vía VPN

Una VPN es una red para transmisión de datos de manera privada, utilizando una infraestructura de telecomunicaciones pública. Se garantiza la privacidad de los datos que viajan por la red, mediante el uso de "túneles de seguridad" a través de Internet.

De esta manera, en las entidades se puede crear una red entre dispositivos que se encuentran localizados geográficamente distantes que es el caso de módulos y delegaciones.

Una de las características más importantes es que garantizar la seguridad de las comunicaciones, mediante autenticación de las sesiones cliente, integridad de los datos y la confidencialidad en los mismos.

Así, se podría seguir trabajando como si todos los equipos informáticos estuvieran conectados a la misma LAN.

Posteriormente sustituir las líneas Frame-Relay e integrar todos los equipos a la VPN.

Se debe de usar según las necesidades de la empresa, ya que de no ser necesaria estaría dentro del plan de contingencia, el cual debe prever los momentos en los que existan contingencias en las cuales quede prohibido salir de casa.

La VPN debe de contar con:

- Conexión a Internet
- En caso de ser Site to Site tener un router que tenga protocolo Ipsec.
- Un usuario y un password para cada empleado
- Limitar el copiado de archivos al equipo remoto
- El acceso de la VPN debe de ser permanente en caso de que se requiera, en caso contrario, en la VPN deben de estar desactivados los usuarios que no la requieran en ese momento para evitar un mal uso de esta.
- La VPN puede ser solicitada mediante la autorización del jefe inmediato y del directivo del área y deberá contar con el visto bueno del área de redes.
- La VPN debe de ser móvil y site to site.

3.7.7. Administración Informática

La administración de la informática debe supervisar e implementar estos puntos mediante las diversas acciones que realiza, tales como:

- Solicitud de equipos
- Actualización de sistemas
- Administración de los recursos de TI

En base a el gobierno de la TI existente y que se adecue al objetivo y visión de la empresa, con el fin de mejorar el rendimiento que se tiene en ella.

a) Administración en redes

Son técnicas que beneficiaran a mantener la red de la entidad eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Entre los puntos más importantes se contemplaran:

- Mejorar la continuidad de la red con elementos adecuados de control y monitoreo, para la solución de problemas y tener recursos para ello.
- Hacer uso eficiente de la red y utilizar mejor los recursos (ancho de banda, instalación de programas, introducción de virus).
- Reducir costos.
- Hacer la red más segura, salvaguardándola contra acceso no autorizado.
- Controlar los cambios y actualizaciones que se producen en la red para que no interfieran en las labores de los usuarios.
- Además debe realizar diversas actividades, las cuales repercutirán en la comunicación de la empresa con sus diversas áreas y con los clientes por lo que debe tener una adecuada funcionalidad.
- Tendrá la responsabilidad del correcto funcionamiento de los servidores de datos, así como indagar cualquier fallo en la red.
- También tendrá que resolver las diferentes solicitudes de los usuarios de la red tanto interna como externa.

b) Administración de los equipos de cómputo

La administración de los equipos de cómputo recae en el área de soporte técnico, la cual está obligada a la correcta función y distribución de los equipos.

Dentro de la correcta función de los equipos de cómputo se refiere a:

- La aplicación de los perfiles de usuario según la función que este desempeñe
- El correcto funcionamiento general del equipo de computo
- El darle mantenimiento preventivo y correctivo al equipo
- El generar respaldos de los datos periódicamente mediante alguna de las herramientas existentes en el mercado para esto
- Mantener el inventario de los equipos actualizados
- El mantener los equipos de cómputo libres de problemas informáticos
- Hacer una comprobación periódica de los discos
- Realizar pruebas con las actualizaciones de los sistemas para verificar que no existan problemas por inestabilidad.
- Mantener el sistema actualizado para minimizar los problemas
- Administración de los perfiles de usuario local
- Revisar que el equipo este constantemente analizado por medio del antivirus.

3.7.8. Recuperación ante desastres.

Esta recuperación es con el fin de que la entidad continué con sus operaciones en caso de que se interrumpan las actividades debido algún siniestro en cuanto a su información para esto se necesita hacer un plan en caso de que ocurra el cual debe consistir en la organización y debe dar apoyo al mismo.

Donde los usuarios deben reaccionar ante los desastres donde tanto ellos como la gerencia deben de participar para que esta continuidad pueda resultar satisfactoria.

Para lograr lo siguiente se dividió de la siguiente forma:

a) Políticas de Recuperación de los datos.

Las políticas de recuperación de los datos norman el cómo debe de realizarse la recuperación de los datos en la entidad, donde existirán una serie de técnicas que permitan que la recuperación de dichos datos sea lo suficientemente correcta cada vez que se necesite establecer políticas para la recuperación de datos es importante determinar en primer lugar cual ha sido la fuente afectada y cuáles son las razones que han causado la perdida de los datos.

En los proceso de recuperación de datos no siempre puede recuperarse toda la información contenida además es muy importante contar con los elementos necesarios para esto, las políticas deberán arrojar los resultados que se desean obtener, de otra forma no se obtendrá su propósito.

b) Organización y clasificación de responsabilidades.

Se debe identificar el personal para la toma de decisiones en la recuperación y la clasificación depende del tamaño de operación. La clasificación dependerá de las siguientes actividades.

- Instalar hardware en el sitio de recuperación del sistema
- Re-direccionar el tráfico de comunicaciones de la red
- Enviar a los usuarios a la instalación de recuperación
- Reconstruir o sustituir lo dañado dependiendo el caso.
- Coordinar el programa de actividades para usar los sistemas y para el trabajo de los empleados.

c) Alternativas de Recuperación.

Es bueno crear procedimientos de las fallas como se mencionó anteriormente que ocurren en las entidades y en listar en cada una de ellas los métodos y herramientas que se podrán ocupar ante un desastre.

Es bueno probar los planes que se realizan para saber que efectivamente este realiza su objetivo ya que muchos negocios carecen de pruebas. Estas pruebas deben estar empleadas en un periodo donde no afecte la realización de las actividades de los usuarios y así no afectar a la entidad.

Las pruebas deben de realizar las siguientes actividades:

- Comprobar la integridad y la precisión del negocio
- Evaluar el desempeño de los empleados que participaron.
- Que las herramientas y métodos sean fiables
- Comprobar que los equipos que se sustituyan cumplan con los requerimientos.

3.8. MAPEO CON OTROS ESTÁNDARES.

Como hemos visto hasta ahora, el estándar propuesto ofrece una amplia gama de directrices respecto a la administración, ejecución y control de la Tecnología de Información. Este estándar se pueden complementar de forma armoniosa con otras metodologías dentro de los procesos de TI dando como resultado la construcción de un verdadero marco de gestión para las organizaciones de cualquier índole; y con mucha más razón en las entidades donde una adecuada gestión de TI puede significar el desarrollo o estancamiento de su crecimiento.

A continuación se hace un pequeño mapeo de la interrelación de los estándares en forma general, también podremos ver la diferencia que existe del estándar ISO/IEC 27002:2005 y nuestro estándar propuesto, demostrando así que se puede llegar a mejorar a detalle mayor los diferentes dominios y objetivos dentro la seguridad de la información.

COBIT	DOMINIOS DE ITIL V3.	ESTÁNDAR ISO/IEC 27002:2005	ESTÁNDAR PROPUESTO
P01.	• Estrategia de Servicio	• No es abarcada por ISO 27002	• Políticas de protección de datos
P02.	• Diseño del Servicio • Transición del Servicio	• Gestión de Activos • Gestión de las comunicaciones y operaciones • Control de Acceso	• Clasificación y control de Activos • comunicación
P03.	• Estrategia del Servicio • Diseño del Servicio	• Políticas de seguridad • Organización de la seguridad de la información • Gestión de las Comunicaciones y Operaciones • Control de Acceso	• Políticas de protección de datos • Comunicación • Clasificación y control de activos
P04.	• Estrategia del Servicio • Diseño del Servicio • Transición del Servicio • Operación del Servicio • Mejora Continua del Servicio	• Organización de la Seguridad de la Información • Seguridad relacionada a los recursos humanos • Cumplimiento • Gestión de Activos • Seguridad Física y Ambiental • Gestión de la Comunicación y Operaciones	• Clasificación y control de activos • Responsabilidad del personal • Clasificación de los Activos • comunicación

P05.	• Estrategia del Servicio • Transición del Servicio • Operación del Servicio	• Política de Seguridad • Gestión de incidentes de la seguridad de la información	• Políticas de protección de datos • Recuperación ante desastres
P06.	• Estrategia del Servicio • Transición del Servicio • Operación del Servicio	• Política de Seguridad • Organización de la información • Gestión de Activos • Seguridad relacionada a los recursos humanos • Seguridad física y Ambiental • Gestión de las Comunicaciones y Operaciones • Control de Acceso • Mantenimiento de los sistemas de información • Gestión de Incidentes de la seguridad de la información • Cumplimiento	• Políticas de protección de datos • Seguridad Física y del entorno • Clasificación y control de activos • Responsabilidad del personal • Comunicación • Administración informática • Recuperación ante desastres
P07.	• Diseño del Servicio	• Seguridad relacionada a los recursos humanos	• Responsabilidad del personal
P08.	• Diseño del Servicio • Transición del	• Organización de la Seguridad de la información	• Clasificación y control de activos

	Servicio • Mejora Continua del Servicio	• Mantenimiento de los Sistemas de información	• Seguridad Física y del entorno
P09.	• Estrategia del Servicio • Diseño del Servicio • Transición del Servicio • Mejora Continua del Servicio	• Política de Seguridad • Gestión de incidentes de la Seguridad de la información • Gestión de la Continuidad del Negocio	• Políticas de protección de datos • Seguridad Física y del entorno • Recuperación ante desastres
P10.	• Diseño del Servicio • Transición del Servicio • Estrategia del Servicio	• No es abarcada por ISO 27002	• Políticas de protección de datos
A11.	• Estrategia del Servicio • Diseño del Servicio • Transición del Servicio • Operación del Servicio	• Organización de la Seguridad de la información • Seguridad relacionada a los recursos humanos • Gestión de las Comunicaciones y Operaciones • Control de Acceso • Mantenimiento de los Sistemas de información	• Clasificación y control de activos • Responsabilidad del personal • Comunicación • Políticas de protección de datos • Administración informática

A12.	• Diseño del Servicio • Transición del Servicio • Operación del Servicio	• Organización de la Seguridad de la información • Gestión de Activos • Gestión de las Comunicaciones y Operaciones • Control de Acceso • Mantenimiento de los Sistemas de información • Gestión de incidentes de la Seguridad de la información • Cumplimiento	• Políticas de protección de datos • Seguridad Física y del entorno • Clasificación y control de activos • Responsabilidad del personal • Comunicación • Administración informática • Recuperación ante desastres
A13.	• Diseño del Servicio • Transición del Servicio • Operación del Servicio	• Seguridad física y Ambiental • Gestión de las Comunicaciones y Operaciones • Mantenimiento de los Sistemas de información	• Recuperación ante desastres • Comunicación • Administración informática
A14.	• Diseño del Servicio • Transición del Servicio • Operación del Servicio	• Gestión de las Comunicaciones y Operaciones • Gestión de incidentes de la Seguridad de la información	• Comunicación • Seguridad Física y del entorno
A15.	• Diseño del Servicio	• Organización de la Seguridad de la	• Políticas de protección de datos

		información • Gestión de las Comunicaciones y Operaciones • Mantenimiento de los Sistemas de información	• Comunicación
A16.	• Transición del Servicio • Operación del Servicio • Mejora Continua del Servicio	• Gestión de las Comunicaciones y Operaciones • Control de Acceso • Mantenimiento de los Sistemas de información	• Comunicación
A17.	• Transición del Servicio • Operación del Servicio • Mejora Continua del Servicio	• Organización de la Seguridad de la información • Seguridad relacionada a los recursos humanos • Seguridad física y Ambiental • Gestión de las Comunicaciones y Operaciones • Mantenimiento de los Sistemas de información	• Políticas de protección de datos • Comunicación • Responsabilidad del personal • Recuperación ante desastres
DS1.	• Estrategia del Servicio • Diseño del Servicio • Transición del	• Gestión de las Comunicaciones y Operaciones	• Comunicación

	Servicio • Operación del Servicio • Mejora Continua del Servicio		
DS2.	• Estrategia del Servicio • Diseño del Servicio	• Organización de la Seguridad de la información • Seguridad relacionada a los recursos humanos • Gestión de las Comunicaciones y Operaciones • Mantenimiento de los Sistemas de información • Cumplimiento	• Políticas de protección de datos • Comunicación • Responsabilidad del personal • Administración informática
DS3.	• Diseño del Servicio • Operación del Servicio • Mejora Continua del Servicio	• Gestión de las Comunicaciones y Operaciones	• Comunicación
DS4.	• Diseño del Servicio • Operación del Servicio • Mejora Continua del Servicio	• Gestión de la Continuidad del Negocio • Gestión de las Comunicaciones y Operaciones • Organización de la Seguridad de la info.	• Políticas de protección de datos • Comunicación

DS5.	• Diseño del Servicio • Operación del Servicio	• Política de Seguridad • Organización de la Seguridad de la información • Seguridad relacionada a los recursos humanos • Seguridad física y Ambiental • Gestión de las Comunicaciones y Operaciones • Control de Acceso • Mantenimiento de los Sistemas de información • Gestión de Incidentes de la seguridad de la información • Cumplimiento	• Políticas de protección de datos • Comunicación • Responsabilidad del personal • Administración informática • Recuperación ante desastres
DS6.	• Estrategia del Servicio • Diseño del Servicio • Operación del Servicio	• No es abarcada por ISO 27002	• No es abarcada por el estándar propuesto
DS7.	• Operación del Servicio	• Seguridad relacionada a los recursos humanos	• Responsabilidad del personal
DS8.	• Operación del Servicio • Mejora Continua	• Gestión de Incidentes de la seguridad de la información	• Clasificación y control de Activos

	del Servicio	• Gestión de Continuidad del Negocio	
DS9.	• Estrategia del Servicio • Transición del Servicio • Operación del Servicio	• Cumplimiento • Gestión de Activos • Gestión de las Comunicaciones y Operaciones • Control de Acceso • Mantenimiento de los Sistemas de información	• Clasificación y control de Activos • Comunicación • Responsabilidad del personal • Administración informática
DS10.	• Operación del Servicio • Mejora Continua del Servicio	• Gestión de Incidentes de la seguridad de la información • Seguridad física y Ambiental • Gestión de las Comunicaciones y Operaciones • Mantenimiento de los Sistemas de información • Cumplimiento	• Comunicación • Administración informática • Recuperación ante desastres
DS11.	• Diseño del Servicio • Operación del Servicio	• Seguridad física y Ambiental • Gestión de las Comunicaciones y Operaciones • Mantenimiento de los Sistemas de información	• Comunicación • Recuperación ante desastres

DS12.	• Diseño del Servicio • Transición del Servicio • Operación del Servicio	• Organización de la Seguridad de la información • Seguridad física y Ambiental	• Políticas de protección de datos • Seguridad Física y del entorno
DS13.	• Diseño del Servicio • Operación del Servicio	• Seguridad física y Ambiental • Gestión de las Comunicaciones y Operaciones	• Seguridad Física y del entorno • Comunicación
ME1.	• Diseño del Servicio • Operación del Servicio • Mejora Continua del Servicio	• Gestión de las Comunicaciones y Operaciones	• Comunicación
ME2.	• No es abarcado por ITIL	• Política de Seguridad • Organización de la información • Gestión de las Comunicaciones y Operaciones • Cumplimiento •	• Políticas de protección de datos • Comunicación
ME3.	• No es abarcado por ITIL	• Organización de la información • Cumplimiento	• Políticas de protección de datos

ME4.	• Estrategia del Servicio • Diseño del Servicio • Mejora Continua del Servicio	• Política de Seguridad • Organización de la información • Gestión de las Comunicaciones y Operaciones	• Políticas de protección de datos • Comunicación

Tabla 3: Mapeo general de Cobit, ITIL V3, ISO 27002 y nuestro estándar propuesto
Fuente: Elaboración propia.

Como se puede notar en la tabla anterior, el estándar propuesto es perfectamente integrable y aplicable con otras metodologías y estándares, de tal forma llegando a reemplazar al estándar ISO/IEC 27002:2005, reduciendo los dominios, objetivos de control y controles de esta, que si se pudieran aplicar de forma armoniosa dentro las entidades, estamos frente a una óptima, eficiente, segura y confiable gestión tecnológica de la información.

3.9. BENEFICIOS.

Hoy en día todas las entidades están en constante comunicación con distintos puntos para lo cual requieren contar con tecnología de punta de manera rápida, eficiente, segura e ininterrumpida para poder realizar operaciones correspondientes a su giro.

Las entidades públicas o privadas requieren tener una fiabilidad en sus comunicaciones con módulos del 100 %, esta comunicación es la base principal para que tengan un buen funcionamiento.

Esta creación del estándar le permitirá a las entidades obtener los siguientes beneficios:

- Contar con un alto nivel de fiabilidad y seguridad en la conexión debido a que entre los dos puntos de comunicación está el Internet por lo que existe un sin número de rutas para establecer la comunicación.

- Contar con un enfoque integral, incluyendo tanto acceso a Internet y arquitectura de Seguridad entre otros.
- Realizar una optimización de los servicios de Internet del grupo.
- Contar con una reestructuración de los enlaces actuales, aplicaciones e infraestructura que brindan los servicios de Internet.
- Exceder los niveles de servicios que hoy en día se tienen.
- Contar con un equipo de seguridad para proteger a la red de datos y la red de servicios públicos contra accesos no autorizados y actos de intrusión por personas maliciosas.
- Contar con un equipo de seguridad escalable que permite su integración con muchos productos de seguridad del mercado.
- Administración personalizada.
- Contar con un esquema de seguridad que le permita soportar los requerimientos no solo actuales sino también futuros.
- Armar las bases para lograr a corto plazo una homogeneidad tanto normativa como tecnológica.
- Optimizar los costos.
- Crear conexiones de Red Virtual entre el esquema de seguridad principal y los equipos adyacentes (VPN's) que mejoren el nivel de seguridad en la confidencialidad de información de la organización.
- Mejor atención al ciudadano
- Concientización de los usuarios antes y después de que ocurra un desastre.

CAPÍTULO 4. CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

Al haber concluido la investigación del presente trabajo se han realizado todas las actividades y los objetivos que se propusieron de manera satisfactoria al principio de la investigación y las conclusiones a las que se llegaron son las siguientes:

- Utilizando el método científico y como base en varias normas de seguridad y calidad para construir la presente metodología la hipótesis planteada es verdadera, con lo cual se demuestra la veracidad de la afirmación.
- En cuanto al seguridad, podemos decir que la metodología ITIL v3. es bastante amplia en cuanto a las tareas prácticas de seguridad y su adecuación dentro de una organización, ya que tiene un proceso dedicado exclusivamente a este fin.
- El Ingeniero que utilice esta metodología, podrá evaluar el contenido y alcance de las distintas fases y aplicar los controles que considere necesario para el objeto de su trabajo.
- De acuerdo a la investigación realizada, la legislación Boliviana no comprende una regulación específica para las metodologías de seguridad.

4.2. RECOMENDACIONES

En nuestro país, existen entidades u organizaciones que cuentan con una administración particular dada su naturaleza. Estas organizaciones públicas y privadas, en su mayor parte cuentan con personal o departamentos encargados del manejo técnico-informático, pero muchas de estas no cuentan con políticas gerenciales que apoyen en la seguridad. Esto genera desconfianza por parte de la gerencia o los propios empleados de la importancia de los departamentos de sistemas.

A partir de estas consideraciones las recomendaciones que se pueden dar a partir del desarrollo de la investigación y pruebas son las siguientes:

- Capacitar al personal de las unidades o departamentos de sistemas en temas de seguridad de información, políticas y normas de calidad en el desarrollo de aplicaciones.
- El trabajo de investigación que se realizó abre nuevas perspectivas de investigación en otras áreas del conocimiento legal informático, como el perito informático, firma digital, etc. Que tienen que ser estudiadas en base al alcance de la doctrina comprada y adaptación a la realidad nacional.
- Mejorar la norma propuesta a través de una implementación más amplia de la metodología ITIL en su tercera versión, dada su evolución y constante mejora.

BIBLIOGRAFÍA

LIBROS

[Marina, 2009]. Jesús Marina Márquez, Seguridad de la información versus Itil V3, año 2009.

[Ramírez, 2006]. Pía Ramírez Bravo, Metodología ITIL, 90 páginas, año 2006.

[Donoso, 2006]. Felipe Donoso Juárez, Metodología ITIL Descripción, Funcionamiento y Aplicaciones, 90 páginas, año 2006.

[Osiatis, 2010]. Formación Itil Versión 3 Fundamentos de la Gestión de Servicios TI, 20 páginas, año 2010.

[Scambray, 2002]. Scambray Joel, Hackers, Editorial McGraw-Hill, España 2002.

[García, 2008], ¿ITIL V2, ITIL V3 o ISO 20000?, año 2008.

[Pérez, 2007]. Alejandro M. Pérez Sánchez, ISO/IEC 20000 el estándar para la Gestión de Servicios TI, 20 páginas, año 2007.

[Cougias, 2009]. Cougias Dorian, "Herramientas de Protección y Recuperación de datos", Editorial ANAYA, año 2009.

DIRECCIÓN WEB

[www, 1].

http://seguridadinformacioncolombia.blogspot.com/search/label/ITIL

[www, 2]

www.itsmf.es

[www, 3].

http//itil-iso 27001-20000convergenciaitilconsgsi.mht.

[www, 4].

http://itsencial-elvalordelatecnologia.blogspot.com/

[www, 5].

http://www.aenor.es/desarrollo/normalizacion/normas/buscadornormas.asp

[www, 6].

http://seguridadinformacioncolombia.blogspot.com/2010/08/alineando-cobit-41-itil-v3-e-iso-27002.html

[www, 7].

http://www.sitographics.com/dicciona/p.html

[www, 8].

http://es.wikipedia.org/wiki/ISO/IEC_17799

[www, 9].

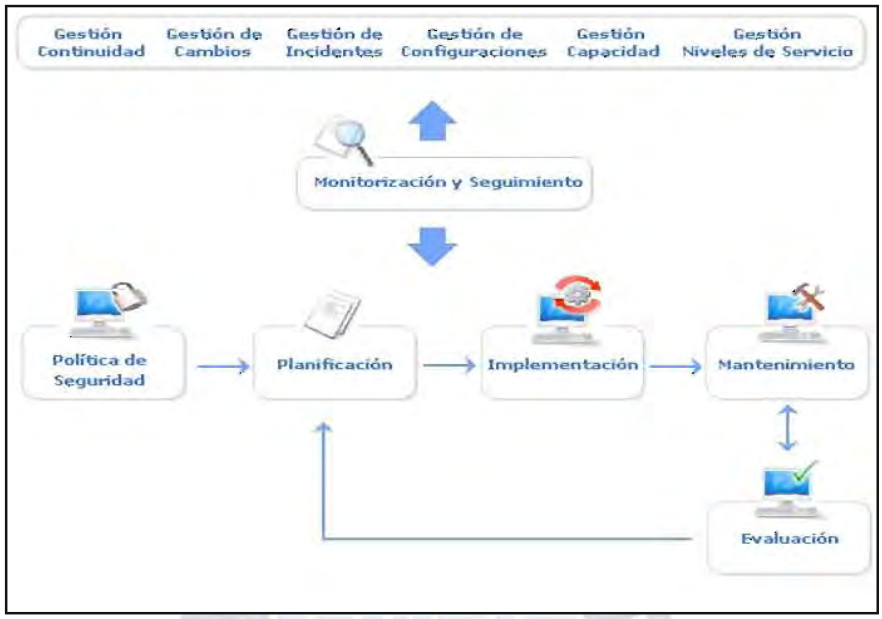
http://www.recuperadata.com

ANEXOS

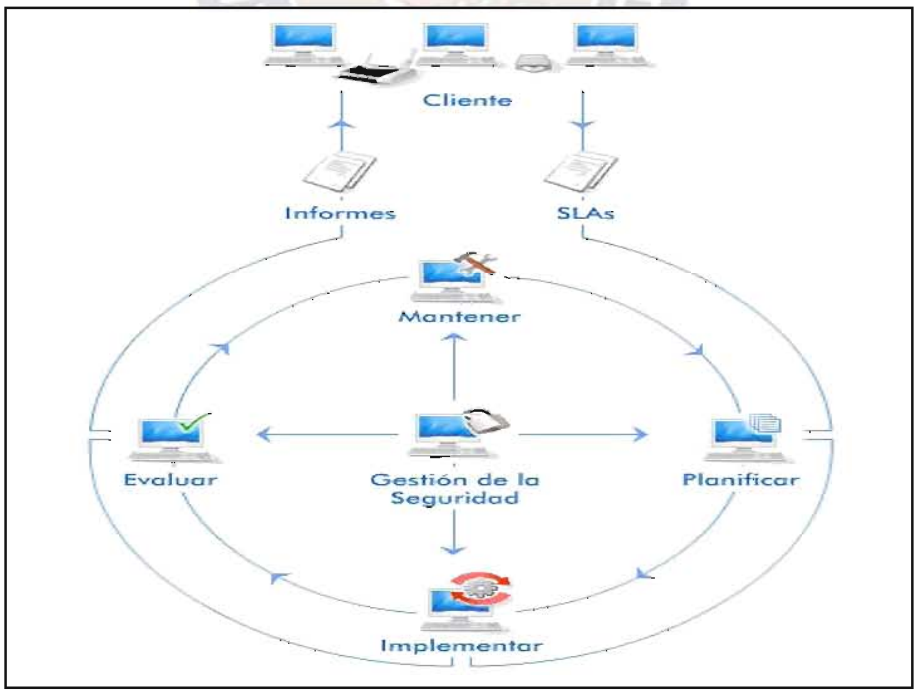
ANEXOS 1: METODOLOGIA ITIL.

PROCESOS DE CERTIFICACION ITIL

LAS INTERACCIONES Y FUNCIONES DE LA GESTIÓN DE LA SEGURIDAD.



OBJETIVOS DE LA GESTIÓN DE LA SEGURIDAD.



ANEXOS 2: ACRÓNIMOS.

AEI Arquitectura e Integración
ASL Biblioteca de servicios de aplicativos
BI Business Intelligence
BSI British Standard Institute
CAM Capacity and Availability Management
CAR Causal Analysis and Resolution
CCTA Computer and Telecommunications Agency
CM Configuration Management
CMF CMMI Model Foundation
CMMI Capability Maturity Model Integration
CMMI-DEV Capability Maturity Model Integration for Development
CMMI-SVC Capability Maturity Model Integration for Services
COBIT Control Objectives for Information and related Technology
COCOMO Constructive Cost Model (Modelo Constructivo de Costes)
CPM Cost Per Thousand impression
CRC Clase-Responsabilidades-Colaboración
CSI Continual Service Improvement
DAR Decision Analysis and Resolution
DCU Diseño Centrado en el Usuario
DFD Diagrama de Flujo de Datos
DSDM Dynamic Systems Development Method
DSL Biblioteca de Software dEFINITIVO

EI External Input
ELF External Logical File
EO External Output
EQ External Queries
GRC Gestión de la Relación con el Cliente
ICASE International Council of Associations for Science Education
IEC International Electrotechnical Commission
IFPUG International Function Point User Group
ILF Internal Logical File
IPM Integrated Project Management
IPO Interacción Persona Ordenador
IRP Incident Resolution and Prevention
IS Ingeniería del Software
ISO International Organization for Standardization
ISPL Biblioteca de adquisición de servicios de información
ITIL Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnologías de Información)
ITSCMM IT Service Capability Maturity Model
ITSM Information Technology service management
IU Ingeniería de la Usabilidad
MA Measurement and Analysis
MOF Microsoft Operations Framework
MSF Microsoft Solutions Framework
OGC Oficina de comercio gubernamental'
OID Organizational Innovation and Deployment
OPD Organizational Process Definition
OPF Organizational Process Focus
OPP Organizational Process Performance
OT Organizational Training
PAR Producto, Facturación, Plataformas Afines a Red
PCR Planeación y Consecución de Recursos
PF Puntos Función
PHVA Planificar-Hacer-Verificar-Actuar
PMC Project Monitoring and Control
PO Puntos Objetos
PP Project Planning
PPQA Process and Product Quality Assurance
PS Prestación de Servicios
PYMES Pequeñas y Medianas Empresas
QPM Quantitative Project Management
REQM Requirements Management
ROI Return On Investment
RRHH Recursos Humanos
RSKM Risk Management
SAF Sistemas Administrativos y Financieros

SAM Supplier Agreement Management
SCON Service Continuity
SD Service Desk
SD Service Delivery
SEI Instituto de Ingeniería del Software
SIP Plan de Mejora del Servicio
SLA Service Level Agreement
SMF Simple Machines Forum
SSD Service System Development
SST Service System Transition
STSM Strategic Service Management
TCO Coste Total de Propiedad
TI Tecnología de la Información
TIC Tecnologías de Información y Comunicación
VSC Ventas y Servicio al Cliente

ABSTRACT

The purpose of this project is the creation of a new standard to apply a protection within an entity or organization to obtain benefits. Everything this based in the present-day and problematical situation of our country. That's why ITIL V3 accomplished an investigation of the methodology and of standards ISO to initiate the proposal, with the aim of helping the Entities by means of analysis coming to the conclusion that the problem shows up.

Himself I evaluate the way of protecting the information at the entities giving as a result several holes that affect the safe informational transfer, besides found various techniques to recover the information and also to preserve them from during analysis these. One found a great variety of implementations that encompass part of what suggested in this standard in the techniques of protection of the data.

Conscious he created of this situation a model of standard establishing a protection to the data of comprehensive way taking the proposal that way for himself that it is gotten there to be a guide that preserves the more important assets from a company data are which and being comprehensive since you foresee making in the event these preventive measures happen causing a bigger minimization of the prostitute of the data.

The model is divided into several points, which go from the administration of them YOU to the user's responsibility, stressing the activities of the information-technology address, they are not which respectively on the subject of techniques or tools to do an effective protection, rather they are focused on the information-technology culture that the employee has.

KEYWORDS: *Informational certainty, Gestión on duty, Itil V3, Itil V2, Cobit, ISO/IEC 27000, ISO/IEC 20000, Question of Services TI, TIC, Seguridad Perimetral, Public Entities, Private Entities, CMD, SLA, Methods of data retrieval, Firewall, Corruptions in the net, protective Technologies.*

INDICE DE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO 1. MARCO REFERENCIAL

En este capítulo se presenta a manera de presentación los antecedentes del trabajo de implementación para la seguridad de la información, la definición del problema, sus objetivos, la hipótesis que buscamos demostrar y por ultimo sus alcances y aportes para el desarrollo del trabajo.

1.1. PRESENTACION

Los Sistemas de Información (SI) y las Tecnologías de Información (TI) han cambiado la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, ya que automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implantación logra ventajas competitivas.

Las Tecnologías de la Información han sido conceptualizadas como la integración y convergencia de la computación, las telecomunicaciones y la técnica para el procesamiento de datos, donde sus principales componentes son: la información, el equipamiento, el factor humano, la infraestructura, el software y los mecanismos de intercambio de información, los elementos de política y regulaciones, además de los recursos financieros. [www, 1].

Los negocios tienden a tener una mayor dependencia de las Tecnologías de la Información. Los departamentos de Sistemas de Información y las actividades en ellos desarrolladas han sido tradicionalmente vistos como un área de soporte al negocio, descuidando incluso muchas veces el uso de criterios racionales para medir su rentabilidad, eficacia y la calidad del servicio ofrecidos a toda la organización. [Donoso, 2006].

Information Technology Infraestructure Library (ITIL), es una metodología que se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos que cubren las actividades más importantes de las organizaciones en sus Sistemas de Información y Tecnologías de Información. Esta metodología fue desarrollada a petición del Gobierno del Reino Unido a finales de los 80 y recoge las mejores prácticas en la gestión de los Sistemas de Información. Desde entonces se ha ido extendiendo su uso en toda la empresa privada, tanto multinacional como PYME, llegando a ser considerado un estándar de facto para la gestión de esta área de la empresa. [Donoso, 2006].

En un entorno donde los periodos de disponibilidad de los servicios son cada vez más amplios, donde las exigencias del cliente son cada vez más elevadas, donde los cambios en los negocios son cada vez más rápidos, es muy importante que los Sistemas de Información estén adecuadamente organizados y alineados con la estrategia del negocio. ITIL propone la gestión de estos Sistemas mediante 10 procesos, con un claro enfoque a la Gestión del Servicio. Igualmente ITIL, ofrece toda una serie de definiciones de conceptos típicos de los Sistemas de Información para garantizar que todos sus conocedores hablen de lo mismo, reduciendo así los tiempos y riesgos por malas interpretaciones. [Ramírez, 2006].

A medida que las redes pasan a ser un elemento integral de las corporaciones, las tecnologías de seguridad de red se desarrollan para proteger datos y preservar la privacidad. El test de seguridad en una red permite identificar vulnerabilidades y asegurar los requisitos de seguridad de cualquier empresa. El análisis de la seguridad permite reconocer información maliciosa, tráfico no autorizado, vulnerabilidades de dispositivos o de la red, patrones de intrusión, y extraer conclusiones de la información recopilada en el test. Entonces, ¿dónde está el problema? Uno de los grandes logros de la versión 3 es haber elevado las TI a los altares de la empresa, situándolas en el nivel estratégico.

Como consecuencia de ello ITIL ha dejado de ser un acrónimo de uso corriente exclusivamente entre los responsables de sistemas y/o seguridad para pasar a formar parte del léxico habitual de la dirección. [Marina, 2009].

En este sentido lo que se plantea en este trabajo es implementar políticas de gestión de cambios adecuadas que evite o al menos controle los cambios no autorizados. En otras palabras se contempla el diseño de servicio apropiados e innovadores, incluido su arquitectura, procesos, políticas y documentación, dentro el departamento de sistemas en entidades públicas, para alcanzar los requerimientos actuales y futuros acordados.

Uno de los pilares centrales de ITIL, la Base de Datos de la Gestión de Configuraciones (CMDB: Configuration Management Data base) juega un papel primordial en este sentido habida cuenta que permite seguir el rastro de todos los componentes TI y mantener la relación entre ellos. CMDB se convierte así en una pieza clave para poder gestionar el servicio dentro de los parámetros de seguridad y calidad fijados.

ITIL v3 va un poco más lejos al incorporar los conceptos de Sistema de Gestión de la Configuración (CMS: Configuration Management System) – conjunto de repositorios que soportan la gestión de la configuración- y de Sistema de Gestión del Conocimiento (SKMS: Servicie Knowledge Managament System). [Marina, 2009].

1.2. ANTECEDENTES

En la actualidad no existen proyectos y/o tesis de grado en la carrera de informática en la que intervenga la metodología ITIL, ya que es una metodología desconocida y que recientemente se está incorporando en nuestro medio dentro las organizaciones para organizar y fundar las mejores prácticas de la gestión de servicio TI.

Los negocios ya no son como hace años, las organizaciones han cambiado y se necesita destacar en la calidad de los servicios TI. En el mundo de las TIC ahora se

está empezando a implantar las mejores prácticas ITIL para optimizar el uso de los recursos informáticos, alineando los objetivos específicos de seguridad con los objetivos generales del negocio. Y el primer paso es que la dirección asuma su responsabilidad, que puede llegar incluso al ámbito legal, en la protección de los activos de su empresa.

Es importante reconocer que las I.T. (Tecnologías De Información) no pueden estar implementadas en una organización ya sea pública o privada, sin que ella esté articulada al diseño estratégico de la empresa; para ello se debe contar con un modelo de diseño estratégico de negocios. [www, 2].

Dentro del modelo de buenas prácticas ITIL, y centrándose en seguridad TIC, la Gestión de la Seguridad es de vital importancia, se contempla en forma de proceso y también participa en la entrega del Servicio. ITIL no solo aporta beneficios a la gestión del servicio TI, también ayuda y facilita a la Gestión de la Seguridad.

Ésta, se relacionada con prácticamente todos los otros procesos TI y necesita para su éxito, la colaboración de toda la organización. Los procesos ITIL "Gestión de la Continuidad del Servicio TI" y "Gestión de la disponibilidad", protegen el grado de disponibilidad de los activos de la información. Los demás procesos, facilitan la ejecución de otras actividades de la Gestión de la Seguridad tales como el tratamiento de incidencias de seguridad, clasificación, implantación de controles a través de la gestión de cambios, gestión de la configuración y gestión de la entrega. [www, 3].

Es necesario realizar también, un control del proceso para asegurar que la Gestión de la Seguridad cumpla con sus objetivos. Si se realiza una correcta Gestión de la Seguridad:

- Se reducen el número de incidencias relacionadas con la seguridad.

- Los accesos a la información de la empresa, serán eficaces y solo por el personal autorizado en base a los parámetros de confidencialidad, integridad y disponibilidad.
- Se identificaran vulnerabilidades antes de que estas se manifiesten y provoquen un problema en la calidad del servicio ofrecido.

Por lo tanto, si se toman medidas a tiempo, minimizaremos la probabilidad de que afecten directamente a nuestro negocio y que nos causen un daño importante.

Hay que tener en cuenta que ITIL es aplicable de manera moldeable a cualquier organización. Esto no es rígido, ya que son una serie de buenas prácticas. Hay que tener bien definido en que terreno nos encontramos actualmente, procesos, estructura organizacional, etc. con tal de definir la mejor estrategia de negocio. La versión 3 de ITIL interactúa mayor mente con la gestión de procesos, por lo que hay que tener en cuenta un control total sobre nuestras acciones, para no llegar a un punto donde nuestra productividad aumente pero con una disminución total en nuestra calidad. [www, 4].

1.3. DEFINICIÓN DEL PROBLEMA

Actualmente nos encontramos con la enorme paradoja de que los mayores recursos humanos y económicos se han venido dedicando a combatir la amenaza externa, descuidando por el contrario la amenaza interna, cuando es esta última la que más quebraderos de cabeza provoca en materia de seguridad. ¿Cuántas veces lo que era aparentemente un sencillo cambio en la configuración de la infraestructura interna o la rutinaria creación de un nuevo perfil de usuario han provocado fallos dejando al descubierto la vulnerabilidad de nuestra política de seguridad? Hemos invertido sobradamente en seguridad perimetral (cortafuegos, sistemas de monitorización y detección de intrusión, control de acceso, etc.) que nos protege del exterior pero no hemos sido igual de cautos (o previsores) a la hora de vigilar y controlar los cambios en la infraestructura TI. La realidad es que nadie puede entrar sin nuestro permiso y

conocimiento pero casi cualquiera puede cambiar la configuración al no tenerla definida.

Las metodologías y normas desarrolladas para combatir las amenazas tanto internas como externas dentro de una entidad u organización llegan a ser muy complejas para su incorporación e implementación dentro de estas, y mucho más para organizaciones pequeñas puesto que les es difícil adecuar estas metodologías a sus estructuras.

Los procesos con la que cuenta la metodología ITIL V.3 pueden ser adecuados a cada situación y cada organización o entidad por parte de los profesionales o personal encargado de la seguridad de los sistemas informáticos, brindando soporte en el diseño estratégico, articulado a los procesos de negocios y los procesos corporativos, en el que debe integrarse y articularse lo gerencial, lo estructural, lo individual y lo institucional; siempre ellos soportados en bases de datos de sistemas de información.

A raíz de los estudios realizados sobre el funcionamiento interno actual dentro de entidades públicas, se han detectado diversos problemas:

- El sistema de infraestructura de tecnologías de la información y comunicación sigue un patrón de comportamiento reactivo ante los problemas que va surgiendo.
- Los mecanismos de funcionamiento de no están bien organizados y esto provoca que los mismos problemas o incidencias se repitan, no haya un tiempo estándar establecido para resolver los mencionados problemas, etc.
- Las diferentes personas que trabajan con los sistemas TIC no tienen bien delimitadas sus funciones, y esto provoca problemas a la hora de resolver problemas en el sistema y a la hora de atender las incidencias que los clientes nos hagan llegar. De esta forma, cualquier circunstancia ante la cual haya que actuar difícilmente será cubierta por la persona más indicada para ello.

- Al no ser capaces de detectar de forma eficiente los problemas en nuestro sistema, ni tampoco de registrarlos de forma ordenada y consciente, no se tienen bases para medir los niveles de calidad que nuestros proveedores nos dan, y por lo tanto de poder reclamar justificadamente el nivel de calidad de servicio contratado, defendernos de posibles engaños, etc.

- No es capaz de establecer un nivel de calidad de servicio y cumplirlo de forma garantizada.

- Al haber tanta heterogeneidad de recursos (plataformas y sistemas operativos diferentes, móviles y PDAs con conexión a Internet, variedad de aplicaciones dedicadas y otras genéricas, telefonía sobre IP prevista para un futuro, acceso cableado e inalámbrico a la red, oficinas distribuidas, etc.), se hace muy compleja la gestión del sistema por el hecho de no disponer de un sistema de gestión totalmente integrado.

Ante la existencia de estos problemas se construye la pregunta de investigación.

¿La incorporación de la metodología ITIL V.3 dentro las normas diseñadas para el manejo de los activos de las unidades de sistemas, solucionara el problema de amenazas externas e internas?

1.4. JUSTIFICACION

1.4.1. Justificación Teórica

Al existir varias Metodologías referidas u orientadas a la seguridad Informática hace dificultosa la elección y la aplicación de alguna de estas en una organización que hace uso de software para realizar el control de tráfico y el comportamiento de la información al interior de estas y en sus diversas áreas donde se toma en cuenta las

aplicaciones que brindan seguridad en sus procesos. Este hecho dificulta la comprensión, aplicación e implementación por parte de los profesionales y los miembros de las organizaciones que se encargan en realizar este tipo de control. Este trabajo de investigación sobre la implementación de los procesos Metodológicos de ITIL V.3 para la seguridad informática, aporta con información para brindar una mayor comprensión sobre el manejo de servicios a través del ciclo de vida, por medio de estrategia, transición, operación y mejoramiento continuo.

1.4.2. Justificación Social

Al implementar los procesos de la metodología ITIL V.3 dentro la estructura de las entidades públicas, se podrá diseminar las mejores prácticas en la gestión de seguridad de la Información de forma sistemática. Por otra parte este trabajo de investigación beneficia a estudiantes, profesionales y personas que quieran tener un mejor acercamiento de Gestión de Negocio y de Gestión de Servicio TI, su razón toma forma de funciones y procesos que busca mejorar el nivel o calidad de servicio comenzando por la planificación pasando por su utilización y seguimiento.

1.4.3. Justificación Económica

El principio de esta metodología está especialmente desarrollada para reducir los costos de provisión, soporte de los servicios de TI, en el momento de combatir amenazas tanto internas como externas y ver el impacto sobre las políticas de seguridad existentes, es decir al dar valor añadido a la gestión de seguridad de la información podremos controlar y evaluar mejor nuestros recursos tecnológicos y económicos.

1.5. OBJETIVOS

1.5.1. Objetivo General

Incorporar dentro la documentación y normas diseñadas específicamente para las unidades de sistemas los procesos basados en la metodología ITIL V.3 para la

gestión de seguridad y servicios TIC que asista y que permita identificar amenazas y riesgos existentes en las unidades de sistemas de las en entidades u organizaciones.

1.5.2. Objetivos Específicos

- Realizar el diseño de la estrategia servicio dentro las organizaciones.
- Aplicar procedimientos que tiendan a evaluar componentes de apreciación del riesgo, ambiente de control, actividades de control y supervisión.
- Analizar y comprobar el funcionamiento de control interno para establecer lineamientos de trabajo en las unidades de sistemas.
- Hacer énfasis en la aplicación de la metodología ITIL V.3 para el desarrollo de las actividades, que permitan evaluar y minimizar los riesgos futuros.

1.6. HIPOTESIS

Es posible ajustar la Metodológica ITIL V.3 con la finalidad de obtener tareas y procesos encerradas en una norma que colabore al área de sistemas, mejorando la seguridad de la información dentro de las unidades informáticas tomando en cuenta el impacto que estos producen a la organización.

1.6.1. Identificación de Variables

Variable independiente: La metodológica ITIL V.3 a ser implementada en los procesos de seguridad de la información dentro las unidades informáticas de las entidades.

Variable dependiente: Todos los componentes TI. en explotación (en funcionamiento).

1.7. ALCANCES Y APORTES

1.7.1. Alcance

El presente trabajo de investigación propone el diseño de estrategias y de gestión de servicios dentro la documentación de procesos de las unidades de sistemas, las cual está basada en la metodología ITIL V.3 dentro de las entidades, aplicando normas para reducir la vulnerabilidad de estas.

La información de esta investigación puede ser de utilidad para las unidades de sistemas de las organizaciones y de personas interesadas en la aplicación de normas de seguridad y los procesos que intervienen esta.

1.7.2. Aportes

Los aportes presentados por este trabajo están principalmente orientados a brindar solución a la falta de normas en el manejo de la información donde intervienen las TIC. Por lo que más de presentar otra norma, lo que se quiere que sea es una herramienta en el manejo de la información.

De esta manera este trabajo proporciona aportes al área de seguridad de la información y manejo de las TIC.

1.8. METODOLOGIA

1.8.1. Métodos y etapas de la Investigación Científica

El método de investigación científica identifica varios tipos de desarrollo que se adecuan a los propósitos que persigue una investigación. En este trabajo de investigación se realizara sobre los lineamientos de la investigación científica experimental, que basa su razón en el uso de una variable experimental no comprobada, en condiciones rigurosamente controladas, con el fin de describir de qué modo o la causa se produce una situación o acontecimiento particular. Las etapas que se establecen para este trabajo son:

- Elección del tema de Investigación
- Identificación y definición del problema
- Definición de hipótesis y variables
- Diseño de plan experimental
- Prueba de confiabilidad de datos
- Realización de experimento
- Tratamiento de datos

CAPÍTULO 2. MARCO TEÓRICO

En este capítulo se analiza el tema de la Seguridad de la Información, análisis de la metodología ITIL, su definición, objetivos, técnicas, y los pasos que se deben seguir en las tareas de Gestión de los Servicios TI y las normas con las que trabaja.

2.1. SEGURIDAD DE LA INFORMACIÓN.

La información es lo que se conoce como un activo. Un activo es un elemento que tiene valor para una organización.

La información, además, puede ser un activo tangible o intangible. Es decir, no solamente tenemos que pensar en información almacenada en los ordenadores o en un disco duro. La información también podemos encontrarla en formato papel, en una cinta magnética, en un CD o en una nota colocada encima de la pantalla de nuestro ordenador.

¿Por qué es valioso un activo para una organización? La respuesta está en la propia organización. Si nos fijamos en una organización cualquiera, vemos que la información que es importante para una organización es relevante para su actividad ya que en torno a ella se crean y desarrollan un conjunto de procesos y tareas. Sin la información, esos procesos y tareas no sirven de nada y no es posible llevarlos a cabo adecuadamente. [Inteco, 2008].

La información, además de las características comentadas, posee otras que determinan la forma en que la utilizamos, y por supuesto, la protegemos. La información proviene de diversas fuentes y se presenta en distintos soportes. Además, la información se transmite a través de distintos medios y tecnologías.

Asimismo, hay que ser conscientes de que la información tiene un ciclo de vida, es decir, durante el tiempo que la información es utilizada pasa por un conjunto de

fases: se crea, se difunde, se transmite, se copia, se modifica, se almacena y, a partir de un momento determinado, deja de ser útil o se convierte en información obsoleta, lo que supone su archivado o destrucción, con lo que llegamos al final de su ciclo de vida. [Inteco, 2008].

A partir de todo lo anterior, estamos en disposición de definir, de una forma comprensible, qué es la Seguridad de la Información.

La Seguridad de la Información es la protección de tres aspectos o facetas de la información, que son las siguientes:

- Confidencialidad: consiste en evitar que personas, programas o sistemas no autorizados puedan acceder a ella sin autorización.
- Integridad: es la característica de la información relativa a su fiabilidad. Su protección consiste en que la información no sea alterada o modificada sin autorización.
- Disponibilidad: este aspecto hace referencia a que la información esté accesible, es decir, disponible para su utilización cuando sea necesaria.

2.1.1. La Seguridad de la Información desde el punto de vista del negocio.

La Seguridad de la Información abarca múltiples aspectos de una organización, no se trata únicamente de cuestiones técnicas, sino también de aquellas relativas a cuestiones organizativas, de procedimiento, de políticas, de responsabilidad, etc.

Por otro lado, la Seguridad de la Información no es competencia exclusiva de los responsables de sistemas de una organización sino que todos los miembros de una organización tienen parte de responsabilidad en mantener un adecuado nivel de seguridad.

Vamos a conocer cuáles son los aspectos fundamentales de las organizaciones sobre los que la Seguridad de la Información nos puede ayudar a mejorar nuestra organización. Como vamos a ver, son básicamente tres:

- La responsabilidad y la productividad.
- La imagen y la competitividad.
- La capacidad para superar contingencias y la continuidad del negocio.

Estos tres grandes grupos engloban la mayoría de los aspectos relativos a cualquier organización en los cuales la Seguridad de la Información nos puede ser de gran ayuda a la hora de mejorarlos. [Inteco, 2008].

2.1.2. La Seguridad de la Información desde el Punto de Vista de las Amenazas.

Para comprender con más claridad el contenido del presente subtitulo avancemos algunos conceptos sobre los tipos de amenazas que existen y que vamos a ver a lo largo de este apartado.

- Subculturas. Hackers, phreakers, hacktivistas, etc. Son el origen de muchas amenazas TIC y es necesario conocer su existencia.
- Malware. Virus, troyanos, ad-ware, keyloggers, etc. Es la base de múltiples técnicas y amenazas. Algunos de ellos llevan con nosotros desde el nacimiento de los ordenadores hasta la actualidad.
- Ingeniería social. Spam, fraude bancario, robo de identidad, etc. Se ha convertido en una de las amenazas principales del uso de las tecnologías de la información e internet. Es la base para múltiples delitos e incidentes de seguridad.
- «El enemigo está dentro». Hasta hace poco se consideraba que la mayoría de las amenazas provenían del exterior de las organizaciones pero cada vez se producen más incidentes de seguridad cuyo origen es la propia organización.

Lamentablemente, las organizaciones criminales han pasado a sustituir a aquellos hackers por algo mucho más siniestro y peligroso. Hoy en día los grupos de

delincuencia organizada han encontrado en internet una nueva frontera para cometer delitos.

Las organizaciones y las empresas se han convertido en nuevos focos de incidentes de seguridad poniendo a sus propios empleados en el punto de mira. Se ha acuñado la expresión «el enemigo está dentro» para referirse a este fenómeno.

Estos cuatro grupos no son más que una de las múltiples formas en las que podemos agrupar las amenazas TIC que existen en la actualidad. [Inteco, 2008].

2.2. DIFERENCIA ENTRE DATO E INFORMACIÓN.

Los datos describen únicamente una parte de lo que pasa en la realidad y no proporcionan juicios de valor o interpretaciones, y por lo tanto no son orientativos para la acción. La toma de decisiones se basará en datos, pero estos nunca dirán lo que hacer. Los datos no dicen nada acerca de lo que es importante o no. A pesar de todo, los datos son significativos para las organizaciones, ya que son la base para la creación de información.

A diferencia de los datos, la información tiene significado (relevancia y propósito). No sólo puede formar potencialmente al que la recibe, sino que está organizada para algún propósito. Los datos se convierten en información cuando su creador les añade significado. Se transforman los datos en información cuando se les añade valor en varios sentidos. Hay varios métodos:

- Contextualizando: Se conoce el para qué propósito se generaron los datos.
- Categorizando: Se conocen las unidades de análisis de los componentes principales de los datos.
- Calculando: Los datos pueden haber sido analizados matemática o estadísticamente.
- Corrigiendo: Los errores se han eliminado de los datos.

- Condensando: Los datos se han podido resumir de forma más concisa.

2.3. PROTECCIÓN DE DATOS.

"Medidas de prevención del uso indebido e indiscriminado de los datos personales contenidos en bases de datos." [www, 7].

Esta definición, genera una idea general de lo que se define como protección de datos, pero no se usará esa definición, ya que está muy limitada a lo que son simplemente las bases de datos, por lo que resultaría excluyente de los archivos planos que utilizan los bancos e instituciones financieras para el procesamiento de datos.

Sin embargo, se utilizará esa definición como base para plantear lo siguiente:

La protección de datos se refiere a las medidas de prevención del uso indebido e indiscriminado de los datos, contenidos en sistemas informáticos.

Habrá de delimitar a los sistemas informáticos ya que esta investigación se enfoca al área informática.

En el intento por proteger los datos, se han creado normas y regulaciones para mejorar la protección de los datos y definir también que es lo que se debe de proteger.

Uno de los más grandes problemas fue solucionado por la Ley Orgánica de Protección a los Datos (LOPD) ya que entre sus regulaciones define qué tipo de dato es privado y cual de acceso público, de manera general.

2.4. RECUPERACIÓN DE DATOS.

Antes de hablar de recuperar datos, es necesario conocer por que debiera recuperarse un dato, esto es debido a que siempre que se generé información existirá por lo menos una entrada de carácter humano, por lo cual al tratarse de

personas, siempre ex iste un nivel de incertidumbre que varía conforme a la confianza, experiencia y valores de esta.

La recuperación de datos se da a partir de la perdida de estos. Esta pérdida se puede deber a diversas causas, y puede conllevar a diversos métodos para su recuperación la cual en la mayor parte de los casos.

Existen diversos factores que pueden ocasionar la necesidad de recuperar información tales como el borrado no intencionado de archivos por un error "de dedo", o "el descubrimiento de que el ordenador tenía un virus que mi antivirus no elimino", o detalles como este que a todos nos ha pasado.

La recuperación de datos es el conjunto de métodos y herramientas para recuperar los datos que contienen la información necesaria para realizar alguna tarea.

2.5. PERDIDA DE DATOS.

Algunas veces cuando se trabaja en extensos proyectos o escritos, como este, en donde se hacen participes más de una persona y se envían archivos mediante las diversas técnicas de comunicación existente, se expone al riesgo de perder información valiosa en la que se ha invertido tanto tiempo y esfuerzo, esto ya sea por algún virus de reciente manufactura, o se encontraba uno cansado y pego mal el documento con la sección A en la sección C y la B en la sección A haciendo un verdadero desorden en su trabajo. [Scambray, 2002].

Muchas veces al corregir estos errores, se ha "perdido" información debida a la falta de algún dato que no está, o se le olvido guardar el documento y su procesador de palabras, no auto guardó esos cambios.

Muchas veces y muchas personas se han encontrado con algún caso parecido, si es que no idéntico al mencionado anteriormente, a esto se le llama

simplemente la perdida de información, pero ¿realmente se pierde la información o se pierden datos?

La ausencia total o parcial de la representación simbólica, atributo o característica de una entidad en un sistema informático es lo que se definirá como perdida de datos.

2.6. CAUSAS DE PÉRDIDAS DE DATOS

Una causa es un factor causante de, en este caso es el factor causante de la perdida de los datos.

Las causas de la pérdida son variadas y probablemente muy distintas entre sí, ya que hay demasiadas maneras de dañar o extraviar datos, entre ellas se engloban las más comunes:

- Desastres Naturales
- La intrusión de algún Hacker o virus
- El error humano
- Falla en el hardware
- Falla en el software

Que son los más comunes y engloban la mayor parte de las causas de pérdida de información. [Scambray, 2002].

2.6.1. Desastres Naturales

La naturaleza se encuentra en un proceso permanente de movimiento y transformación, que se manifiesta de diferentes maneras, a través de fenómenos de cierta regularidad como la lluvia, los temblores, erupciones volcánicas y otros eventos que llegan a ocasionar daños tales como las inundaciones, deslizamientos de tierra, incendios.

En esta categoría de desastres naturales están todas aquellas causas que están fuera de nuestra capacidad para evitarlos, tales como el incendio de la oficina donde está el servidor, o los movimientos telúricos de la tierra, los tsunamis, inundaciones y las fallas eléctricas.

Esta última no es un desastre natural, pero está fuera de nuestra capacidad para evitar la pérdida de datos. [Scambray, 2002].

2.6.2. Errores Humanos

Esta categoría esta creada por todos las posibles causas debidas a la actividad humana, que para nuestra investigación resulta la más común, ya que por la condición humana se tiende a cometer pequeños incidentes que causan la perdida de datos, como por ejemplo el olvidar salvar el documento antes de dejar el equipo o guardar este archivo en el CD regrabable que prestaste antes de entregar a revisión.

También se debería englobar toda aquella actividad que intencionadamente cause la perdida de datos, mas sin embargo por tratarse de algo intencional se ha separado para tratar estos problemas de forma separada y sea más sencillo el metodizarlos. [Scambray, 2002].

2.6.3. Hackers

En esta categoría se encuentran todas aquellas actividades en la que interviene un tercero utilizando diversas técnicas para el robo de información y para causar un daño en el sistema informático.

Entre estos agentes están los “hackers”, programas de auto propagación tales como virus, gusanos, caballos de Troya y todo aquel software que perjudique a los equipos de cómputo.

2.6.4. Falla de Hardware y Software.

La falla de Hardware y Software es otra de las categorías más comunes, si es que no una de las principales causas de la perdida de datos.

La falla de software no es más que la posible secuela de la recuperación del sistema después de un ataque informático (virus, etc.) y que ha dejado rastros de su ataque alterando el correcto funcionamiento del sistema. También está el cuelgue del sistema operativo o del mismo sistema, definiendo como cuelgue de sistema cuando la computadora aun responde y nuestro programa queda pasmado.

El cuelgue del sistema operativo es una falla aún más grave ya que conlleva a la detención de todo programa o sistema ejecutado en el equipo que sufrió dicho percance, haciendo en algunos casos más difíciles la detección de la perdida de datos y su recuperación.

Las fallas de Hardware son debidas a problemas físicos, principalmente se da en los medios de almacenamiento tales como memorias, discos duros, y medios de almacenamiento móvil.

2.7. ITIL V3.

ITIL puede ser definido como un conjunto de buenas prácticas destinadas a mejorar la gestión y provisión de servicios TI. Su objetivo último es mejorar la calidad de los servicios TI ofrecidos, evitar los problemas asociados a los mismos y en caso de que estos ocurran ofrecer un marco de actuación para que estos sean solucionados con el menor impacto y a la mayor brevedad posible.

Sus orígenes se remontan a la década de los 80 cuando el gobierno británico, preocupado por la calidad de los servicios TI de los que dependía la administración, solicito a una de sus agencias, la CCTA acrónimo de Central Computer and Telecommunications Agency, para que desarrollara un estándar para la provisión eficiente de servicios TI.

En la actualidad es la OGC (Office of Government Commerce) el organismo encargado de velar por este estándar y la responsable de la última versión de ITIL (v3) que data del año 2007. [Osiatis, 2010].

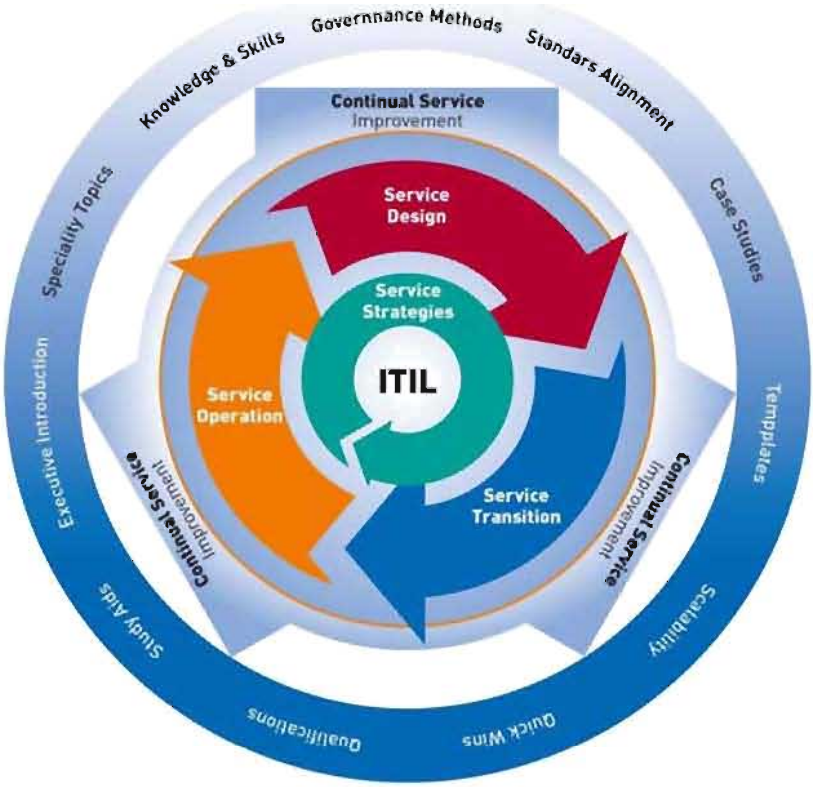


Figura1: La infraestructura ITIL.
Fuente: "Fundamentos de Itil V3." Ricardo Adrián Federico.

La OGC cuenta con la colaboración de varias organizaciones para el mantenimiento de ITIL:

- **itSMF:** El Information Technology Management Forum es una organización independiente y reconocida internacionalmente que tiene como principal objetivo impulsar la adopción de las mejores prácticas ITIL para la gestión de servicios TI.

- **APM Group:** Es una organización comercial encargada por la OGC de definir, publicar y gestionar las certificaciones ITIL así como de acreditar a los organismos examinadores.
- **Organismos examinadores:** En la actualidad existen varios organismos examinadores acreditados por APMG entre los que se encuentran EXIN, BCS/ISEB y LCS.

2.7.1. Gestión de Servicios TI.

La tecnología de la información es tan antigua como la historia del hombre y está a jugado gran papel en la misma. Pero, no ha sido hasta tiempos recientes que por medio de la automatización de su gestión que se ha convertido en una herramienta imprescindible y clave para organizaciones y empresas.

Hoy en día nadie duda de que la información es el recurso estratégico más importante que tiene cualquier organización y que para que la organización proporcione servicios TI de alta calidad es fundamental que se realice un análisis, producción y distribución de la información que maximicen dicha calidad.

La concienciación de que los servicios TI son cada vez más importantes para el negocio ha llevado a la introducción de la gestión de servicios TI. La gestión de servicios TI está dirigida a proporcionar datos para la toma de decisiones desde una perspectiva de procesos, y proporcionar una implementación profesional con responsabilidades bien definidas. Un prerrequisito de las organizaciones es una disposición incondicional tanto de dirección como del personal TI para centrarse en el cliente y en el servicio.

La gestión de servicios TI está compuesta por un conjunto de capacidades organizacionales especializadas para proporcionar valor a los clientes en forma de servicios. Tales capacidades incluyen funciones y procesos utilizados para gestionar los servicios a través de su ciclo de vida, con especializaciones en estrategia, diseño,

transición, operación y mejora continua. El acto de transformar recursos en servicios con valor es el centro de la gestión de servicios.

2.7.2. Objetivos Gestión de Servicio TI.

Los objetivos de una buena Gestión de Servicio TI han de ser:

- Alinear los servicios TI con las necesidades del negocio y sus clientes
- Mejorar la calidad de los servicios TI
- Reducir el coste en la provisión de servicios

2.7.3. El Ciclo de Vida de los Servicios TI.

ITIL v3 estructura la gestión de los servicios TI sobre el concepto de Ciclo de Vida de los Servicios.

Este enfoque tiene como objetivo ofrecer una visión global de la vida de un servicio desde su diseño hasta su eventual abandono sin por ello ignorar los detalles de todos los procesos y funciones involucrados en la eficiente prestación del mismo. [Business, 2009].

El Ciclo de Vida del Servicio consta de cinco fases que se corresponden con los nuevos libros de ITIL:

- Estrategia del Servicio: propone tratar la gestión de servicios no sólo como una capacidad sino como un activo estratégico.
- Diseño del Servicio: cubre los principios y métodos necesarios para transformar los objetivos estratégicos en portafolios de servicios y activos.
- Transición del Servicio: cubre el proceso de transición para la implementación de nuevos servicios o su mejora.
- Operación del Servicio: cubre las mejores prácticas para la gestión del día a día en la operación del servicio.