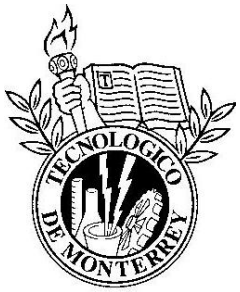
Instituto Tecnológico y de Estudios Superiores de Monterrey

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS EN ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES



MODELO DE ADMINISTRACIÓN DE SEGURIDAD DE INFORMACIÓN PARA PROCESOS BÁSICOS DE TECNOLOGÍA DE INFORMACIÓN BASADO EN MARCO DE TRABAJO DE ITIL Y EL ESTÁNDAR ISO/IEC-17799

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADÉMICO DE:

MAESTRÍA EN CIENCIAS EN TECNOLOGÍA INFORMÁTICA

POR

Rubí Shelby Jaramillo Islas

MONTERREY, N.L. DICIEMBRE 2004

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

DIVISIÓN DE ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES

PROGRAMA DE GRADUADOS EN ELECTRÓNICA,COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES

Los miembros del comité de tesis recomendamos que la presente tesis de la Ing. Rubí Shelby Jaramillo Islas sea aceptada como requisito parcial para obtener el grado académico de **Maestro en Ciencias en Tecnología Informática**.

Comité de Tesis

M. en C. Ricardo Morales González
Asesor Principal

Dr. Jorge Carlos Mex Perera
Sinodal

M. en C. Daniel Mijares Valles
Sinodal

Dr. David A. Garza Salazar
Director del Programa de Posgrado en Electrónica, Computación, Información y Comunicaciones
Diciembre de 2004

MODELO DE ADMINISTRACIÓN DE SEGURIDAD DE INFORMACIÓN PARA PROCESOS BÁSICOS DE TECNOLOGÍA DE INFORMACIÓN BASADO EN MARCO DE TRABAJO DE ITIL Y EL ESTÁNDAR ISO/IEC-17799

POR

RUBÍ SHELBY JARAMILLO ISLAS

TESIS

Presentada al Programa de Graduados en Electrónica, Computación, Información y Comunicaciones

Este trabajo es requisito parcial para obtener el grado de Maestro en Ciencias en Tecnología Informática

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

DICIEMBRE 2004

DEDICATORIA

A Dios:

Mi Padre celestial, fuente inagotable de sabiduría, fortaleza y amor porque lograr esta meta es una prueba más de tu presencia en mi vida.

A mi Papá:

De cuyo ejemplo de amor, integridad y trabajo he recibido mi formación personal y anhelo de superación. Gracias por tu esfuerzo a lo largo de mi vida, realmente tengo en tí una persona muy especial y sé que no hace falta tenerte frente a mí para saber que estas a mi lado y que no podría haber logrado este meta sin tu apoyo.

A mi Mamá:

Una mujer triunfadora, comprensiva, capaz de hacer sentir lo bello de esta vida, que está a mi lado brindándome su apoyo, su guía y sobre todo su amor. Por haber hecho de mí lo que soy, por mostrarme con su ejemplo el valor de la disciplina, el amor y sobre todo por enseñarme lo verdaderamente importante: Amar a Dios, por quererme como tú solo sabes hacerlo y por saber que en tí, tengo mucho más que una amiga y más de lo que puedo desear en la vida.

A mi hermanos:

Con mucho cariño y como estímulo para que logren alcanzar todas las metas que se propongan.

Con profundo Amor y Eterno Agradecimiento

AGRADECIMIENTO

Quiero agradecer especialmente al Dr. Carlos Mex Perera, por su valioso apoyo, tiempo, disposición y por orientarme acertadamente para la culminación exitosa de la presente tesis, por ser un buen profesor y una excelente persona.

Al M.en C. Ricardo Morales González por darme la oportunidad de desarrollar mi tesis en un tema tan interesante.

Al M. en C. Daniel Mijares Valles, por el interés mostrado en esta tesis y por sus aportaciones.

Índice general

Índice de tablas

Índice de figuras

Capítulo 1

Introducción

En la actualidad las empresas son conscientes de la gran importancia que tiene el desarrollo de sus actividades con el hecho de proteger de forma adecuada su información y en especial aquella que les permite realizar correctamente su actividad de negocio. El poder gestionar de manera adecuada la seguridad de la información no sólo permitirá garantizar, que los recursos de la organización tiene un alto nivel de protección, sino que también asegurará la confidencialidad, integridad y disponibilidad de los mismos, lo cual les aportará a los clientes un grado de confianza superior al que puedan ofrecer sus competidores, convirtiéndose en un factor significativo de distinción en el competitivo mercado en el que la empresa desarrolla su comercio.

En un principio se consideraba que las empresas debían protegerse de lo externo, de los peligros de Internet, pero con el paso del tiempo se ha observado que no sólo existen este tipo de amenazas sino que también hay peligros dentro de la organización y que éstos deberían ser contemplados a la hora de realizar un plan de seguridad.

Debido a la necesidad de asegurar la información era preciso la existencia de algún estándar que englobase todos los aspectos que una organización debe considerar para proteger sus activos de información de manera eficiente, frente a los probables incidentes que pudiesen afectarla, ante esta disyuntiva el Instituto de Estándares Británico (BSI, *British Standard Institute*) publicó el estándar BS-7799 en 1995. Este documento fue presentado a aprobación por la Organización Internacional de Estándares (ISO, *International Standard Organization*) para adoptar un estándar internacional de seguridad de la información. En el año 2000, la ISO publicó una versión internacional del BS-7799, conocido como ISO/IEC-17799.

El ISO/IEC-17799 considera a la organización como una totalidad, así como también todos los aspectos que se ven afectados ante los posibles incidentes que pueden suceder. El estándar se encuentra estructurado en 10 dominios en los que cada uno de ellos hace referencia a un aspecto de la seguridad de la organización, los cuales se tratarán más a detalle en las siguientes secciones de este trabajo.

Aunado a esto, los ambientes de Tecnología de Información (en lo sucesivo *TI*) llegan a ser complejos y como consecuencia, la administración y la seguridad de la infraestructura llega a ser crítica, ya que los procesos del negocio cada vez dependen más de la Tecnología de Información. Debido a esto las organizaciones se vuelven a estándares que les ayuden a implementar "mejores prácticas", las cuales dan a las organizaciones una forma de estandarizar sus procesos y administrar sus ambientes de TI. El marco de trabajo líder en esta área es la Librería de Infraestructura de Tecnología de la Información ($ITIL^{®}$, *Information Technology Infrastructure Library*) la cual es un marco de trabajo para procesos de Gestión de Servicios de TI más aceptado en el mundo. $ITIL^{®}$ proporciona un conjunto de mejores prácticas, extraídas de organismos principales del sector público y privado a nivel internacional, que han sido reunidas por la Oficina Gubernamental de Comercio (Británica) (OGC, *Office of Government Commerce*). Este marco de procesos es utilizado por cientos de organizaciones en el mundo y ha sido desarrollado reconociendo la dependencia creciente que tienen éstas en la tecnología para alcanzar sus objetivos. La parte central de la librería esta compuesta de dos volúmenes los cuales son; *Soporte de Servicio y Entrega de Servicios* y que posteriormente se tratan a detalle en este trabajo.

1.1. Objetivos

1. Proponer un modelo de seguridad basado en el marco de trabajo de ITIL y el estándar ISO/IEC-17799 para los siguientes procedimientos de información:
   a) Respaldo de Información.
   b) Registro de Usuarios y Administración de Privilegios.
   c) Controles contra Software Malicioso.
   d) Monitoreo y Registro de Eventos.

2. Proponer normas de seguridad para los procedimientos de TI antes mencionados, las cuales estén basadas tanto en las mejores prácticas determinadas por ITIL y el estándar ISO/IEC-17799.

1.2. Justificación

La información es un activo muy importante en todas las organizaciones y puede existir de muchas formas. Puede ser impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o de manera electrónica. En el ambiente competitivo de hoy en los negocios, esa información está constantemente bajo las amenazas de distintas fuentes, estas pueden ser internas, externas, accidentales o maliciosas. Con el incremento del uso de nueva tecnología para almacenar, transmitir y recuperar información, las empresas están expuestas a un mayor número y tipo de amenazas.

Debido a esto se requiere establecer un programa global de seguridad de la información dentro de la organización. Se vuelve esencial para asegurar la confidencialidad, integridad y disponibilidad de información vital corporativa y la información sobre los clientes. Entre los estándares que proporcionan controles para lograr la seguridad de la información se encuentran; el estándar ISO/IEC-17799 y el marco de trabajo ITIL que se han convertido en marcos ampliamente aceptados de control interno, control informático y control de la seguridad de la información que otorgan credibilidad a los procesos y tecnologías que son necesarios para el soporte de ambientes de procesos del negocio, debido a lo anterior se hace uso de tales estándares en este proyecto de tesis, en los cuales se basan las mejores prácticas y normas de seguridad, creadas para los procesos de seguridad requerido por la empresa Alestra.

Por otra parte el estándar ISO/IEC-17799 prepara a la empresa para que reciba la acreditación de seguridad en los procesos en los cuales será implementado, la cual se realiza a través de una auditoría realizada por un auditor externo a BSI (British Standard Institute) pero acreditado por éste. La acreditación les asegurará a sus clientes y asociados que la información guardada en las redes empresariales está segura y que la seguridad general de la empresa es confiable.

Adicionalmente una empresa certificada con el estándar técnico ISO/IEC-17799 puede tener ventajas frente a los competidores que no están certificados. Si un cliente potencial tiene que escoger entre dos proveedores diferentes y la seguridad es un aspecto importante, generalmente optará por la empresa certificada. Además una empresa certificada tendrá las siguientes ventajas:

- Mejoramiento de la seguridad empresarial
- Planeación y manejo de manera más efectiva de la seguridad
- Protección continua

- Alianzas comerciales más seguras
- Mayor grado de confianza del cliente
- Auditorías de seguridad más precisas y confiables
- Menor Responsabilidad civil

La manera de llegar a ser posible la seguridad de información en una empresa es mediante la aplicación de normas, estándares y procedimientos de seguridad, por lo que en este proyecto de tesis se establecen normas de seguridad basadas en los estándares antes mencionados.

1.3. Hipótesis

1. La identificación de los procesos más relevantes al negocio que se apoyan significativamente en Tecnología de Información más importantes en la empresa ayudan a tener un mejor control y uso de la información.
2. La implementación de Normas de seguridad basadas en el estándar ISO/IEC-17799 y en el ITIL, definen el uso adecuado de la información y determina quien tendrá la responsabilidad de la aplicación del modelo de seguridad.
3. El uso de un modelo de seguridad de información basado en ITIL e ISO/IEC-17799 garantiza un alto grado de confidencialidad, integridad y disponibilidad de la información.

1.4. Alcances

La empresa de Telecomunicaciones Alestra, a través del Área de Seguridad de la Información, ha realizado estudios de Análisis de Riesgos, basados en estándares de gestión y seguridad de información; tales como, el ITIL y el ISO/IEC-17799, en el que de acuerdo al resultado de dichos análisis se ha concluido que los siguientes procedimientos operativos son los de mayor impacto en las propiedades de Confidencialidad, Integridad y Disponibilidad de la Información.

Por lo tanto y de acuerdo a esto, en este proyecto de tesis se establecen normas de seguridad para los siguientes procesos:

1. Respaldo de Información.
2. Registro de Usuarios y Administración de Privilegios.
3. Controles contra Software Malicioso.
4. Monitoreo y Registro de Eventos.

El enfoque de este proyecto de tesis es la creación de normas de seguridad debido a que estas son independientes de la tecnología, no así los estándares y procedimientos, lo cual limitaría la aplicación de las normas aquí establecidas, por lo cual cabe mencionar que estas normas están dirigidas a una empresa de servicios de Telecomunicaciones, tal como lo es Alestra, sin embargo para otras empresas esta tesis representará un marco de referencia para la aplicación adecuada de normas de seguridad a sus procesos de TI antes mencionados.

1.5. Contribución de la Tesis

Actualmente existen estándares de Gestión de Servicios de TI y de Gestión de Seguridad de Información de manera separada, pero no existe ningún modelo o guía que integre los estándares y lo cual permita la emisión eficiente de normas de seguridad para procedimientos específicos de TI.

Por tal motivo, la contribución principal de este proyecto de tesis es el integrar las "mejores prácticas" determinadas por el marco de trabajo ITIL, y los controles de seguridad especificados por el estándar ISO/IEC 17799, a fin de obtener normas que proporcionen un alto nivel de seguridad de la información.

Capítulo 2

Marco Teórico

2.1. Código de Práctica para el Manejo de Seguridad de Información ISO/IEC-17799

El Código de Práctica para el Manejo de Seguridad de Información ISO/IEC-17999 es un conjunto de controles que incluyen las "mejores prácticas" en seguridad de la información, ya que es un estándar genérico reconocido a nivel internacional y cuya principal intención es servir como un punto de referencia único para identificar los controles necesarios en la mayoría de las situaciones en los que los sistemas de información se ven involucrados en la industria y el comercio.

Este código surge como consecuencia de la demanda a nivel internacional de un estándar de calidad que regule la seguridad de la información. La tarea del ISO comenzó con la adopción del BS 7799 (British Standard [BS] 7799), un estándar de calidad de gestión de seguridad de la información nacido inicialmente en 1995, a través del estándar ISO/IEC-17799. El *ISO 17799-1: Code of Practice for Information Security Management*, Código de Práctica para el Manejo de Seguridad de Información. Es una guía para empresas y organizaciones, ya que establece lo que la empresa "debe hacer´´ para contar con una gestión eficaz de la seguridad de la información. Proporciona recomendaciones para el Manejo de Seguridad de Información, así como las bases para desarrollar estándares de seguridad organizacional y la práctica para el manejo efectivo de seguridad.

El ISO/IEC 17799-1 consta de 10 partes esenciales para el Manejo de Seguridad de Información [13], la cuales se mencionan a continuación:

1. Políticas de seguridad. Proporciona la directriz y el soporte de la dirección general de la empresa para la seguridad de la información
2. Clasificación y control de activos. Mantiene la protección adecuada de los activos corporativos y garantizar que los activos informáticos reciban un nivel adecuado de protección.
3. Administración de las operaciones y equipo de cómputo. Evita al máximo el riesgo de fallas en el sistema, incluido el hardware y software.
4. Seguridad de la organización. Administra y mantiene al máximo la seguridad de la información y de las instalaciones de una compañía.
5. Seguridad del personal. Reduce el riesgo del factor humano, robo, fraude, abuso de la información, sistemas y equipos. Asegurarse que el personal esté consciente de las amenazas a la información y sus implicaciones.
6. Cumplimiento. Todos los involucrados deben evitar infringir cualquier norma civil o penal, ley, reglamento, obligación contractual o cualquier requerimiento de seguridad; asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad; maximizar la efectividad y minimizar las interferencias en el sistema.
7. Seguridad física y ambiental. Previene el acceso no autorizado a las instalaciones para evitar pérdida, robo, daño de los bienes o interrupción de las actividades productivas.
8. Desarrollo y mantenimiento de sistemas. Garantiza que la seguridad del sistema esté construida dentro de la aplicación para prevenir pérdidas, abusos y modificaciones de los datos.
9. Sistemas de control de acceso. Control del acceso a la información; previene los accesos no autorizados a sistemas de información; garantiza la protección de servicios de red; impide los accesos no autorizados a las computadoras; detecta actividades no autorizadas; salvaguarda la información cuando se utiliza cómputo móvil o remoto.
10. Planeación de la continuidad del negocio. El objetivo es contrarrestar las interrupciones de las actividades críticas del negocio, así como evitar fallas mayores o desastres.

Como complemento, el contenido del *BS 7799-2: Specification for Information Security Management Systems,* Especificaciones para el Sistema de Administración de Seguridad de Información, lo constituyen 127 controles que la compañía ha de implantar para contar con una gestión de seguridad de información que sea válida. En

ellos se dispone lo que la compañía "tiene que hacer" y, en caso de cumplimiento con lo dispuesto por los citados controles, es posible que la compañía obtenga la certificación.

El ISMS (Sistema de Gestión de Seguridad de Información, en lo sucesivo *SGSI*) esta diseñado para asegurar y proporcionar controles de seguridad que protegan adecuadamente la información y de esta manera dar confianza a los clientes.

El ISO/IEC-17799 promueve la adopción de procesos para el establecimiento, implementación, operación, monitoreo, mantenimiento y mejoramiento efectivo de un SGSI de la organización. Para que una organización funcione eficientemente se deberán de identificar y manejar actividades que harán uso de recursos, cualquier actividad administrada para realizar la transformación de entradas a salidas deberá ser considerada como un *proceso*. Con frecuencia la salida de un proceso forma directamente la entrada del siguiente. La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacción de los mismos, puede se definido como un "enfoque de procesos". [12]

Un enfoque de procesos fomenta a los usuarios a enfatizar la importancia de los siguientes conceptos:

1. Entendimiento de los requerimientos de Seguridad de Información de negocios y la necesidad de establecer políticas y objetivos para la seguridad de la Información.
2. Implementación y operación de controles en el contexto del manejo de riesgos de negocios en las organizaciones.
3. Monitoreo y revisión del cumplimiento y eficiencia del Sistema de Administración de Seguridad de Información (ISMS).
4. Mejora continua basada en la medición de objetivos.

El modelo, que se muestra en la Figura 2.1, es conocido como "Plan-Do-Check-Act" (PDCA) puede ser aplicado a todos los procesos de SGSI como adopción en este estándar.[12]

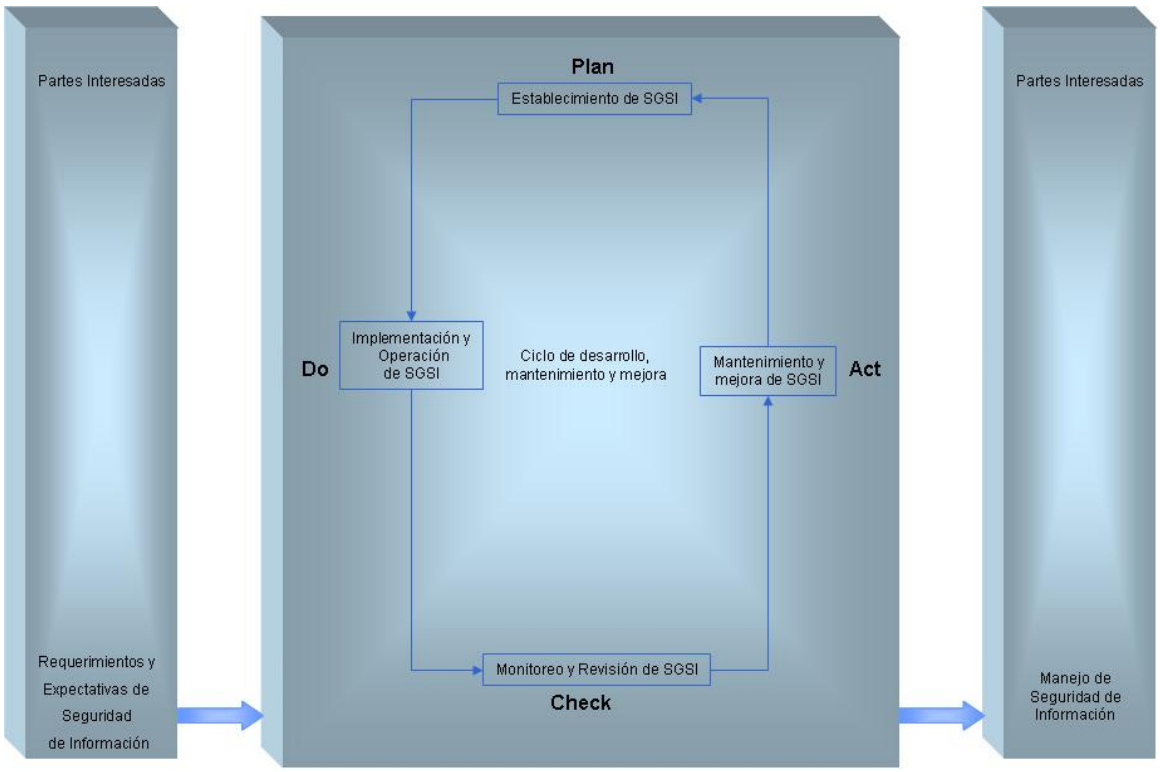


Figura 2.1: Modelo PDCA aplicado a procesos SGSI

A continuación se describen las partes del modelo mostrado en la Figura 2.1.

Plan (Establecimiento de SGSI). Establecimiento de políticas de seguridad, objetivos, procesos y procedimientos relevantes para el manejo de riesgos y mejora de la seguridad de información para comunicar resultados de acuerdo a las políticas y objetivos de la organización.

Do (Implementación y Operación de SGSI). Implementación y operación de las políticas de seguridad, controles, procesos y procedimientos.

Check (Monitoreo y Revisión de SGSI). Evaluación y medición del cumplimiento de los procesos a través de políticas de seguridad, objetivos y experiencias prácticas y reporte de resultados de administración.

Act (Mantenimiento y mejora de SGSI). Tomar acciones preventivas y hyphenationcorrectivas correctivas, basadas en el manejo de revisiones, para lograr mejoras continuas del SGSI.

De acuerdo al ISO/IEC-17799, los aspectos más importantes que la Seguridad de Información debe tener en cuenta son los siguientes:

- Confidencialidad: Se refiere a asegurar que la información sea accesible solamente a quienes tienen acceso autorizado
- Integridad: Salvaguardar la exactitud de la información y los métodos de procesamiento.
- Disponibilidad: Se refiere a asegurar que usuarios autorizados tengan acceso a la información y a activos asociados cuando lo requieran.

2.2. ITIL, Librería de Infraestructura de Tecnología de Información

La Librería de Infraestructura de Tecnología de Información, ITIL (por sus siglas en inglés de Information Technology Infrastructure Library) es un conjunto de "mejores prácticas" para el Manejo de Servicios de Tecnología de Información (TI) que ha sido desarrollado desde 1989. Empezó como un conjunto de procesos usado por el gobierno de Reino Unido con el propósito de mejorar el manejo de servicios de TI y ha sido adoptado por varias empresas. El marco de trabajo tiene como objetivo ser útil para organizaciones de todos los sectores. [6]

La parte central de la librería esta compuesta de dos volúmenes los cuales son: *Soporte de Servicio y Entrega de Servicios*.

El área de *Soporte de Servicios* se refiere a asegurar que el cliente tenga acceso apropiado a los servicios para soportar las funciones de negocio [6]. Los temas discutidos en esta área son los siguientes:

- Administración de la Configuración
- Administración al Cambio
- Administración de la distribución de software
- Manejo de Incidentes
- Manejo de Problemas
- Servicio de Desk

El área de *Entrega de Servicios* se refiere a los requerimientos de negocio por parte del proveedor para proporcionar un soporte adecuado a los clientes [6]. A fin de proporcionar el soporte necesario esta área trata los siguientes temas:

- Administración del Nivel de Servicios
- Administración de la Capacidad

- Administración Financiera de los Servicios de TI
- Administración de la Disponibilidad
- Administración de la Continuidad de Servicios de TI

2.3. Descripción y Relación de Procesos de ITIL

2.3.1. Administración de la Configuración

La administración de la Configuración es una parte integral de todo proceso de Administración de Servicios. En la actualidad la información precisa de todos los componentes en la infraestructura es más eficiente, en particular, en la Administración del Cambio. El proceso de Administración del Cambio puede ser integrado con el proceso de Administración de la Configuración. Toda petición de Cambio debe ser introducida en la Base de Datos de Administración de Configuración (CMDB, Configuration Management Data Base) y registrar las actualizaciones como el progreso de petición a través de la implementación.

El sistema de Administración de la Configuración identifica la relación entre un punto que será cambiado o algún componente de la infraestructura, esto permite a los propietarios de estos componentes ser involucrados en la evaluación del impacto del proceso. Siempre que es realizado un cambio a la infraestructura, es asociado en la CMDB un registro de Administración de Configuración, el cuál deberá ser actualizado.

La CMDB debe estar disponible a un grupo de soporte de servicios para que los Incidentes y Problemas puedan ser resueltos más fácilmente, entendiendo la posible causa de falla del componente. La CMDB también deberá ser usada para enlazar los registros de incidentes y problemas a los registros apropiados tales como el Artículo de Configuración con falla (CI, Configuration Item) y el Usuario.

La Figura 2.2 muestra una relación simple entre los procesos de Administración de la Configuración y otros servicios en el proceso de Administración.

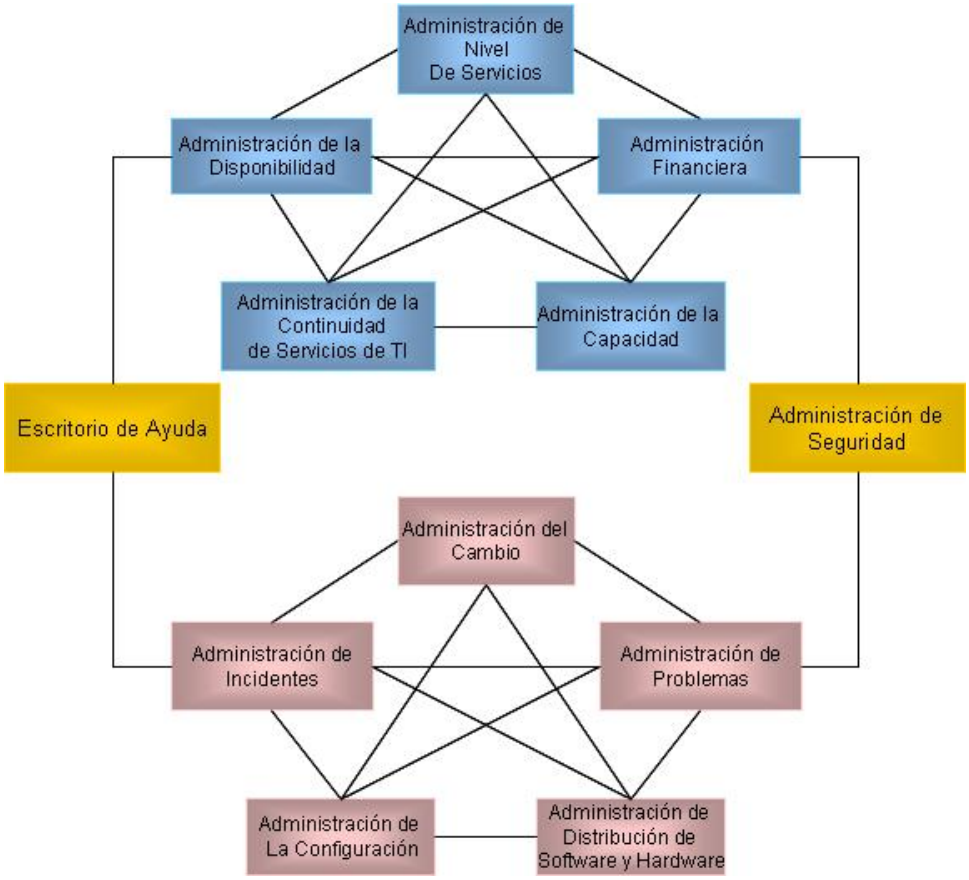


Figura 2.2: Modelo de Relación entre Procesos

2.3.2. Administración del Cambio

Los procesos de Administración de Cambios dependen de la exactitud de la configuración de los datos para asegurar que es conocido el impacto de realizar cambios a la configuración. Por lo tanto, existe una relación muy estrecha entre los procesos de Administración de la Configuración, Administración de la distribución de software y la Administración del cambio.

Los detalles de los procesos de cambio son documentados en los Acuerdos de Nivel de Servicios (SLA, Service Level Agreement), para asegurar que los usuarios conocen los procedimientos de las peticiones del cambio y el impacto de la implementación de dichos cambios.

Los detalles de los cambios debes ser conocidos por el Servicio de Desk. Aun cuando se realicen las pruebas correspondientes pueden ocurrir dificultades después de

la implementación de un cambio. El Consejo Consultivo de Cambios (CAB, Change Advisory Board) es un grupo de personas quienes pueden proporcionar una solución especializada al equipo de Administración del Cambio acerca de la implementación de un cambio. Este equipo esta integrado por representante de diversas áreas de TI [6].

2.3.3. Distribución de Software y Hardware

Los cambios frecuentemente resultan en la necesidad de nuevo hardware, nuevas versiones de software y/o nueva documentación. Los medios para lograr que la distribución de nuevo software y hardware sean distribuidos son los procesos de Administración del Cambio y la Administración de la Configuración. Los procesos de distribución de software puede llegar a ser una parte integral de la Administración de Incidentes y la Administración de Problemas, y por lo tanto también esta estrechamente relacionada con la CMDB con la finalidad de mantener un registro de las actualizaciones del software y del hardware [6].

2.3.4. Manejo de Incidentes

Debe existir una interface cercana entre los procesos de Administración de Incidentes y el de Administración de Problemas con los procesos de Administración de Cambios y la función de Servicios de Desk. Si estos no son controlados apropiadamente, los Cambios pueden introducir nuevos Incidentes. Debe existir una manera de monitorear estos procesos paralelamente, se recomienda que los registros de los incidentes se mantengan en la CMDB junto con los registros de los Problemas y Errores Conocidos para facilitar el reporte o investigación de un incidente ocurrido [6].

La prioridad de los incidentes y los procedimientos de escalación necesitan ser acordados como parte del proceso de Administración del Nivel de Servicio y documentado en los SLAs.

2.3.5. Administración de Problemas

Los procesos de Administración de Problemas requieren un registro exacto y entendible de los incidentes para identificar efectiva y eficientemente la causa y la tendencia de los incidentes. La Administración de Problemas también necesita estar estrechamente relacionado con el proceso de Administración de la Disponibilidad para identificar estas tendencias y determinar una acción que solucione el problema [6].

2.3.6. Servicio de Escritorio de Ayuda

El Servicio de Desk es solamente el punto de contacto entre los proveedores de servicio y los usuarios, es un procedimiento básico día a día. También representa un punto focal para el reporte de Incidentes y realizar peticiones de servicio. El Servicio de Desk tiene la obligación de mantener informados a los Usuarios de eventos de Servicios, acciones y oportunidades que probablemente impactarían a sus actividades diarias.

El Servicio de Desk esta en relación directa con los SLAs y debido a esto se necesita un flujo rápido de información [6].

2.3.7. Administración del Nivel de Servicios

El proceso de Administración de Nivel de Servicios (SLM , Service Level Management) es responsable de asegurar los Acuerdos de Nivel de Servicios (SLAs) y sostener los Acuerdos de Nivel de Operación (OLA, Operational Level Agreement),y asegura que algún impacto adverso a la calidad de servicio sea minimizado. El proceso involucra la evaluación del impacto de los cambios sobre la calidad de servicios y SLAs, en ambas facetas, cuando son propuestos los cambios y cuando son implementados. Uno de los objetivos más importantes es el conjunto de SLAs relacionados a la disponibilidad de servicios y requiere la solución de Incidentes dentro de los periodos acordados [6].

2.3.8. Administración de la Capacidad

La Administración de la Capacidad esta directamente relacionada con los requerimientos del negocio y no simplemente acerca del desempeño de los componentes del sistema, individual o colectivamente. La administración de la Capacidad esta involucrada en la solución de Incidentes y la Identificación de Problemas que están relacionados con cuestiones de capacidad.

Las actividades del proceso de Administración de la Capacidad surgen de una Petición de Cambio (RFC, Request for Change)para asegurar que la capacidad está disponible apropiadamente. Estos RFC están sujetos al proceso de Administración del Cambio, incluyendo hardware, software y documentación los cuales requieren una efectiva Administración de Distribución de software.

La Administración de la Capacidad debe estar involucrada en la evaluación de todos los cambios, para establecer el efecto sobre la capacidad y el desempeño. Esto

debe de ocurrir cuando los cambios son propuestos y después que son implementados. Se debe de poner especial atención a los efectos de los cambios durante un periodo en que están siendo implementados, ya que se pueden combinar efectos negativos causados por los cambios y ocasionar problemas, tales como: fallas en el almacenamiento de archivos, degradación en el tiempo de respuesta y demanda excesiva en la capacidad del procesamiento [6].

2.3.9. Administración Financiera de los Servicios de TI

La Administración Financiera es responsable de la contabilidad para proporcionar servicios de TI y de algunos aspectos de recuperación de estos costos para los clientes. Se requiere al establecimiento de interfaces correctas entre los procesos de Administración de la Capacidad, Administración de la Configuración (datos activos) y Administración del Nivel de Servicios para identificar los costos correctos de los servicios. El Gerente Financiero trabaja muy estrechamente con el Gerente de Relación con el Cliente y con el Director de TI, durante la negociación del presupuesto del departamento de TI y el gasto individual de los Clientes [6].

2.3.10. Administración de la Disponibilidad

La Administración de la Disponibilidad se refiere al diseño, la implementación y la administración de servicios de TI para asegurar los requerimientos del estado del negocio para la disponibilidad. La Administración de la Disponibilidad requiere de entender las razones por las cuales puede ocurrir una falla y el tiempo que toma para resumir los servicios. La administración de Incidentes y la Administración de Problemas proporcionan una entrada clave para asegurar que las acciones apropiadas correctivas están progresando.

Un reporte de disponibilidad de TI asegura que el nivel de disponibilidad entregado satisface lo establecido en los SLAs. La Administración de la Disponibilidad soporta procesos de Administración del Nivel de Servicios, para proporcionar medidas y reportes para el soporte de servicios [6].

2.3.11. Administración de Continuidad de Servicios de TI

La Administración de Continuidad de Servicios de TI se refiere al manejo y a la habilidad de la organización para continuar proporcionando un determinado nivel de Servicios de TI que garantice la disponibilidad de los mínimos requerimientos para que el negocio siga funcionando después de haber ocurrido una interrupción mayor.

La Continuidad de Servicios de TI efectivo requiere un balance entre las medidas de reducción de riesgos, tales como sistemas resistentes a amenazas y opciones de recuperación de información. Es necesaria la información acerca de la configuración de los equipos para facilitar la planeación de la continuidad del negocio en caso de falla de algún equipo.

Es necesario evaluar la infraestructura del negocio para conocer el impacto potencial que se tendría sobre ésta en caso de un incidente y las repercusiones que tendría en la continuidad del negocio [6].

2.4. Documentos relacionados a la Seguridad de la Información

En esta sección se presenta algunos conceptos que deben tomarse en cuenta al desarrollar políticas, normas, estándares, guías y procedimientos de seguridad de información, los cuales son una serie de múltiples documentos interrelacionados que utiliza una organización para administrar y proteger la información de la que depende para sus operaciones actuales y futuras [4]. Desafortunadamente, las discusiones acerca de las "políticas", "estándares" y "procedimientos" para la seguridad de la información con frecuencia no son de pleno consenso; y pueden provocar malos entendidos, información errada y definiciones contradictorias.

Desde la perspectiva de seguridad de la información, éstos términos no están claramente definidos en español y no se traducen fácilmente a otros idiomas. Teniendo en cuenta lo anterior, es importante primero definir los términos prácticos para que puedan ser fácilmente entendidos.

Quizás una ilustración como se muestra en la Figura 2.3 es la mejor forma de imaginar este grupo importante de documentos de protección a la información:

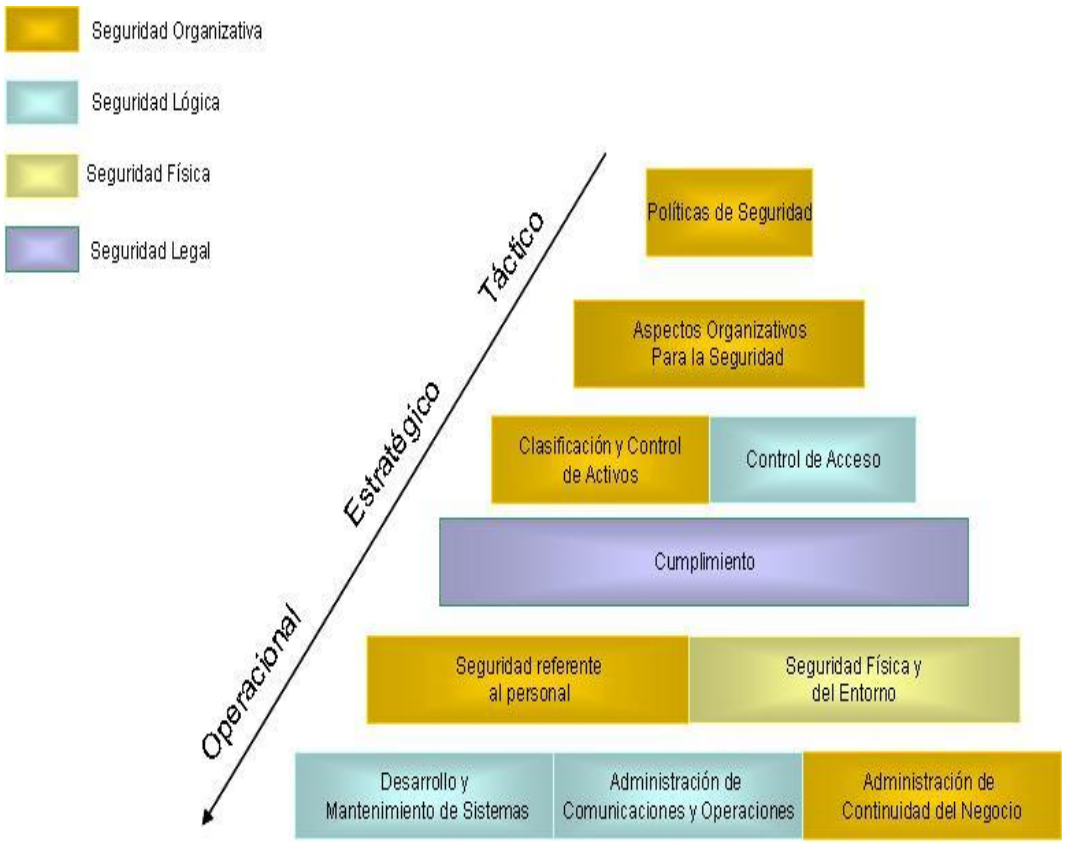


Figura 2.3: Pirámide Seguridad de Información

Es importante aclarar cada uno de los conceptos anteriores, ¿Que se quiere comunicar cuando se dice política, norma, estándar, mejor práctica, guía o procedimiento? A continuación se explica cada uno ellos:

2.4.1. Política

Es una declaración general de principios de directivas de acción que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación durante un periodo prolongado y es de esperar que no sufran modificaciones durante este y que guíen el desarrollo de normas y criterios más específicos que aborden situaciones concretas. La política de seguridad se apoyan e implementan mediante las normas, estándares, mejores prácticas, guías y procedimientos de seguridad de la información. La Política de Seguridad ofrece compromiso y respaldo administrativo para que se brinde protección a la información.

Por definición, todas las políticas son de carácter obligatorio y ante la incapacidad o imposilidad para cumplir una política exige que se apruebe una excepción. [11]

La Dirección de la empresa es responsable de definir y publicar las Políticas de Seguridad como una firme declaración de directivas ejecutivas, así como de divulgarlas en todo el ámbito de la empresa.

Una Política de Seguridad de la Información está conformada generalmente por los siguientes elementos [4]:

- Alcance de aplicabilidad
- Necesidad de adhesión a la política
- Descripción general de la política
- Consecuencias de no adherir a la política

Para que la política sea verdaderamente efectiva, debe ser aprobada y firmada por el director general de la organización. No obtener este compromiso generalmente significa que el cumplimiento de la política es opcional, situación que fracasará en proteger la información adecuadamente.

Una Política de Seguridad de la Información es un documento de ley dentro de la organización. Debe estar escrito desde esta perspectiva y debe evitar terminología jurídica que pueda confundir a la mayoría de las personas. Cuando se redacte la política, es mejor tener el principio de claridad, será más efectivo y aceptable para las personas a las que aplica. Una política típica de seguridad de la información debe tener un máximo de dos páginas.

Características principales de una Política de Seguridad de la Información [4]:

- Debe estar escrita en lenguaje simple, claro y sencillo pero jurídicamente viable.
- Debe basarse en las razones que tiene la empresa para proteger la información.
- Debe ser consistente con las demás políticas organizacionales.
- Debe hacerse cumplir, se exige y mide el cumplimiento.
- Debe tener en cuenta los aportes hechos por las personas afectadas por la política.
- Debe definir el papel y responsabilidades de las personas, departamentos y organizaciones para los que aplica la política.
- No debe violar las políticas locales, estatales o federales.
- Debe definir las consecuencias en caso de incumplimiento de la política.
- Debe estar respaldada por documentos "palpables", como los estándares y procedimientos para la seguridad de la información, que se adapten a los cambios en las operaciones de las empresas, las necesidades, los requerimientos jurídicos y los cambios tecnológicos.

2.4.2. Norma

Basándose en las Políticas de Seguridad, la Dirección de la empresa publicará las Normas de Seguridad, en las que se definirá qué hay que proteger y el objeto concreto de esa protección [11]. Una Norma debe ser breve, concisa y redactada en términos claros y comprensibles por todos los empleados, y debe contener como información de control, al menos:

- Nombre de quien la elaboró
- Nombre de quien la aprueba
- Identificación de la Norma
- Fecha de publicación
- Fecha de efectividad o entrada en vigor
- Fecha prevista de revisión o renovación
- Si es aplicable a toda la empresa o a un ámbito más reducido
- Si sustituye a una norma precedente o es nueva.
- Las Normas son de obligado cumplimiento, por lo que deben ser divulgadas, de acuerdo con su ámbito de aplicación, a todos los empleados involucrados, incluido el personal directivo.

El conjunto de todas las Normas de Seguridad debe cubrir la protección de todos los entornos de los Sistemas de Información de la empresa.

2.4.3. Estándar

Los estándares de seguridad de la información constan de documentos múltiples que se aplican a todas las áreas de la empresa que utilizan la información. Estos estándares abarcan controles de seguridad físicos, administrativos y lógicos (técnicos) que están diseñados para proteger la información. Uno de los documentos de estándares define el contenido y presentación de toda la documentación de seguridad de la compañía de manera que muchas organizaciones contarán con docenas de documentos de los estándares para la seguridad de la información [4].Los Estándares de Seguridad de la Information definen lo que se debe hacer para satisfacer los requerimientos de seguridad especificados en la Política de Seguridad de la Información de la organización.

Un estándar es una regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares sirven como especificaciones para la implementación de las políticas, son diseñados para promover la implementación de las políticas de alto nivel de la organización antes que crear nuevas políticas [3].

Un estándar es una especificación aceptada para hardware, software o acciones humanas. Un ejemplo de estándar técnico es el protocolo TCP/IP que especifica como deben ser interconectados los sistemas dentro de Internet.

Un estándar de Seguridad de la Información, establecen lo siguiente:

- Lo que se debe hacer
- Los controles de seguridad que se requieren
- Controles de seguridad adecuados que se apliquen a cada elemento del entorno de protección de la información

A continuación se mencionan algunos aspectos claves de los estándares [4]:

- Todo Estándar de Seguridad de la Información debe respaldar los objetivos comerciales de la organización, las normas y reglamentaciones que aplican a la empresa y sus operaciones y que son congruentes con otras políticas organizacionales.

- Los Estándares de Seguridad de la Información se deben diseñar para proteger la información y para que los usuarios de la misma realicen sus funciones normales sin tener que hacer esfuerzos irrazonables para acceder a la información que necesitan para ser productivos.
- Los Estándares de Seguridad de la Información deben respaldar únicamente los requerimientos especificados en la Política de Seguridad de la Información. Si se exige el cumplimiento de la Política de Seguridad de la Información, también se exigirá el cumplimiento de los Estándares de Seguridad de la Información relacionados.
- Para que los Estándares de Seguridad de la Información sean efectivos y utilizables , los gerentes de la empresa y los expertos técnicos deben trabajar mancomunadamente para producir los documentos. Esto es importante porque el siguiente nivel de documentación - los procedimientos - deben cumplir totalmente con los requerimientos especificados en estos estándares y respaldarlos.
- La creación de los Estándares de Seguridad de la Información es una tarea tanto comercial como técnica que requiere de la interacción humana para garantizar que los resultados finales satisfagan las necesidades de la empresa y sean aceptados como parte normal de las operaciones de la empresa por parte de las personas para quienes aplican los estándares.
- Lo más importante es que todo Estándar de Seguridad de la Información debe cumplir con los requerimientos de seguridad exigidos por la Política de Seguridad de la Información.

2.4.4. Mejores Prácticas

Es una regla de seguridad específica a una plataforma que es aceptada a través de la organización al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las carac-teristicas de seguridad de sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización [6].

2.4.5. Guía

Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son, esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque

no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo [11].

2.4.6. Procedimiento

Los procedimientos definen específicamente cómo las políticas, normas, estándares, mejores prácticas y guías serán implementados en una situación dada. Los procedimientos son dependientes de la tecnología o de los procesos y se refieren a plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada a dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso de TI o sistema. Los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican [11].

Ni la Política ni los Estándares relacionados definen cómo se deben implementar y administrar los controles de la seguridad. Esta es función de los Procedimientos de Seguridad de la Información; son documentos de uso diario, por los cuales funcionan los gerentes, personal de redes y sistemas, y el departamento de seguridad de la información. Si los procedimientos están adecuadamente trazados para los estándares, la administración del cumplimiento de los requerimientos de seguridad es simplemente cuestión de asegurar que se sigan detalladamente los procedimientos.

Además de desarrollar los procedimientos para implementar los requerimientos especificados en los estándares, se debe desarrollar un proceso para evaluar y permitir excepciones. Estas excepciones (bajo circunstancias muy controladas) permiten el incumplimiento de procedimientos específicos. Es imperativo que se limite estrictamente el tiempo y alcance de dicho proceso para evitar abusos.

Se requieren significativamente más documentos de procedimiento que la cantidad total de documentos de seguridad de la información de nivel superior (la política, las normas y sus estándares relacionados). Los procedimientos están orientados por tareas y cualquier estándar requerirá usualmente que se realicen muchas actividades para lograr el cumplimiento del estándar.

Es típico que los documentos de la Política, las Normas y los Estándares no se modifiquen con frecuencia después de su aceptación inicial. Sin embargo, los documentos de Procedimiento de Seguridad de la Información pueden ser alterados a menudo en entornos computacionales, operativos y comerciales. Es imperativo que se mantengan buenos procesos de administración de cambio de los documentos para estos procedimientos. De hecho, el procedimiento de administración de cambio de los documentos debe ser el primer procedimiento que se documente.

Cada procedimiento debe utilizar un formato y presentación estándar, para que los usuarios que necesiten cumplir con los múltiples procedimientos, no se confundan con los múltiples estilos y presentaciones. Lo ideal es que los procedimientos estén al alcance de los usuarios tanto en formato escrito como electrónico.

Obviamente algunos procedimientos pueden contener información sensible corporativa, para lo cual la accesibilidad debe estar muy controlada. En estos casos, no sería prudente publicar estos documentos en un sitio Web de intranet que no controle el acceso de los empleados (lo que probablemente será prohibido por uno de los estándares) [4].

Elementos recomendados de un Procedimiento [4]:

El siguiente es el esquema de un procedimiento:

- Propósito del procedimiento
  - Qué estándar cumple
  - Cuál es el objetivo del procedimiento
- Alcance del procedimiento
  - A qué sistema(s), red(es), aplicacion(es), personal, instalación se aplica este procedimiento
  - Qué función se espera que este proceso ejecute
  - Los conocimientos previos que se necesitan tener para ejecutar el proceso
- Definición del proceso
  - Introducción al proceso
    - Descripción de lo qué el proceso hace
  - Descripción detallada de:
    - Cómo se ejecutará el proceso

        - Cuándo se ejecutará el proceso
        - Lo que se espera que suceda durante la ejecución del proceso
        - Lo que no se espera que suceda
            - Las acciones que se tomarán si ocurre un hecho imprevisto
        - Qué criterios indican la ejecución exitosa del proceso
        - Qué informe (si existe) se debe suministrar al finalizar el proceso, quién enviará la información y qué información se enviará
        - Las interacciones requeridas o esperadas de otros procesos
- Listas de los procesos
- Problemas de los procesos
    - Qué se hará si se presenta un problema en el proceso
        - Error de proceso
        - Excepción del proceso por no aplicabilidad

Aspectos esenciales para el desarrollo de procedimientos exitosos

Los procedimientos deben estar escritos en lenguaje sencillo para que cualquier usuario pueda entenderlo. Si se necesita utilizar jerga o siglas, se debe adjuntar un glosario al procedimiento y desarrollar un estándar del glosario con todos los términos utilizados en el paquete de documentación de la seguridad.

La elaboración de los Procedimientos de seguridad de la información es una tarea que es desarrollada por o con el personal que ejecutará el procedimiento. Muchas organizaciones han descubierto que las personas que no están involucradas en el desarrollo del proceso por lo general no demuestran "sentido de propiedad" por el proceso y creen que su conocimiento sobre la forma cómo operan los sistemas, no es valioso.

Por consiguiente, este personal está dispuesto a ignorar el proceso y adoptar una actitud de "Yo se más que eso" o "Siempre lo hemos hecho de esta manera", lo que no augura un buen resultado para los departamentos, a los que se les puede hacer auditorias para verificar si cumplen con los procesos aplicables. En el caso de una auditoría, el cumplimiento con los procesos es decisivo y no quien escribió el proceso y si es percibido como correcto o no.

Lo más importante es que cada Procedimiento de seguridad de la información

debe cumplir con los controles de seguridad exigidos por (los) Estándar(es) de Seguridad de la Información importante(s).

Capítulo 3

Propuesta del Modelo de Administración de Seguridad de Información de TI

En esta época no es un secreto la importancia de implementar un programa completo para la seguridad de la información de una empresa. Sin embargo, crear un programa de seguridad con base en los componentes de "bloqueadores de cookies" rara vez produce resultados efectivos. Lo más efectivo es utilizar una metodología que diseñe un modelo de seguridad con base en las necesidades de la empresa.

Es frecuente que las personas involucradas con seguridad de información tengan una visión estrecha de lo que significa desarrollar un modelo de administración de seguridad de información, pues no basta con redactar políticas y pretender ponerlas en práctica. En ocasiones se incluye la asignación de responsables, se realizan actividades para dar a conocerlas y, quizá se supervise su cumplimiento; pero esto tampoco basta. Muchos modelos de seguridad de información fallan ya que se desconoce lo que implica realmente desarrollarlos e implementarlos.

Es importante resaltar que un modelo de seguridad tiene un ciclo de vida completo mientras esta vigente. Este ciclo de vida incluye un esfuerzo de investigación, labor de redactarlo, lograr que las directivas de la organización lo acepten, conseguir que sea aprobado, lograr que sea diseminado a través de la empresa, concientizar a los usuarios de la importancia de las políticas, conseguir que la acaten, darle seguimiento, garantizar que estén actualizadas y, finalmente, suprimirlas cuando haya perdido vigencia. Si no se tiene en cuenta este ciclo de vida se corre el riesgo de desarrollar políticas que sean poco tenidas en cuenta, incompletas, redundantes, sin apoyo por parte de los usuarios y las directivas.

En el caso de este proyecto de tesis se crearán normas de seguridad para diversos procesos información, los cuales se describen más adelante. El modelo que se muestra en la Figura 3.1, muestra el flujo del proceso de seguridad de ITIL, el modelo esta formado por fases, en las cuales los datos de salida de una fase representan los datos de entrada en la siguiente, resultando así en un ciclo. La entrada inicial en este modelo esta determinada por el SLA, el cual es una interpretación de las necesidades de negocio del cliente, los SLAs tratan las demandas de seguridad de información y la manera en la cual estos requerimientos serán planeados e implementados. La seguridad de la información debe ser *controlada, planeada, implementada, evaluada y mantenida* y un *reporte* de status para el cliente cerrará el ciclo.

Figura 3.1: Modelo del Proceso de Administración de Seguridad de Tecnología de Información

A continuación se describe cada una de las fases del modelo.

3.1. SLA, Acuerdo de Nivel de Servicios

EL modelo de Acuerdo de Nivel de Servicios (Service Level Agreement, SLA) consiste en un contrato entre el proveedor de servicios y el cliente, en el que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes, así, refleja contractualmente el

nivel operativo de funcionamiento, penalizaciones por caída de servicio, limitación de responsabilidad por no servicio, etc.

Este modelo no ha de estar relacionado necesariamente con la contratación de servicios a terceras partes, sino que puede implantarse a nivel interno, transformando una determinada unidad de negocio en centro de servicios que provea a la propia compañía.

En esta parte del contrato se describe y obliga a un nivel específico de calidad en el suministro.

Los principales puntos a cubrir deben ser:

- Tipo de servicio.
- Soporte a clientes y asistencia.
- Provisiones para seguridad y datos.
- Garantías del sistema y tiempos de respuesta.
- Disponibilidad del sistema.
- Conectividad.
- Multas por fallo del sistema.

Estos puntos son muy importantes a la hora de formalizar de forma contractual una operación.

Implantación de acuerdos de nivel de servicio con proveedores

Para implantar con éxito un SLA han de tenerse en cuenta un serie de factores clave, de los que va a depender en gran medida la obtención de los resultados deseados:

- **Aspectos críticos**. Los aspectos más críticos, son la definición de procedimientos estándares y los mecanismos de evaluación y seguimiento.
- **En la implantación de un SLA se deben seguir una serie de puntos**
  1. Definición de Objetivos: mejora de la eficacia, reducción de costos, formalizacion de la relación
  2. Identificar expectativas: qué es lo que espera la organización de este acuerdo
  3. Adecuada planificación temporal
  4. Optimización/rediseño de procesos (revisar los procesos si el SLA no asegura ningún cambio o como mínimo formalizarlos)

- Errores más frecuentes en la implantación
  - Definir niveles de servicio inalcanzables
  - Regulación excesiva
  - Error en la definición de prioridades
  - Complejidad técnica
  - Irrelevancia (si un SLA no tiene ningún efecto sobre el cliente, el objetivo no tiene sentido)

3.2. Análisis de Riesgos

En un entorno de información existen una serie de recursos (humanos, técnicos, de infraestructura, etc.) que están expuestos a diferentes tipos de riesgos: los 'normales', aquellos comunes a cualquier entorno, y los excepcionales, originados por situaciones concretas que afectan o pueden afectar a parte de una organización o a toda la misma, como la inestabilidad política en un país o una región sensible a terremotos). Para tratar de minimizar los efectos de un problema de seguridad se realiza lo que denominamos un análisis de riesgos, término que hace referencia al proceso necesario para responder a tres cuestiones básicas sobre nuestra seguridad:

- ¿Qué se quiere proteger?. Definición de la entidad o activo a proteger.
- ¿Contra quién o qué se quiere proteger?. Identificación del agente originador de la amenaza.
- ¿Cómo se quiere proteger?. Definición de las medidas de seguridad.

La Seguridad de la Información tiene como objetivo el mantenimiento de la Confidencialidad, Integridad y Disponibilidad de los Sistemas de Información. Es necesario identificar y minimizar el daño que un evento que pueda causar a cualquiera de estos tres aspectos, así como definir e implantar las defensas necesarias para eliminar o reducir sus posibles consecuencias.

3.2.1. Componentes del Análisis de Riesgos

En un proceso de Análisis de riesgos se pueden establecer los siguientes componentes:

Sistema de Información. Son los Recursos Informáticos y Activos de Información de que dispone la empresa para su correcto funcionamiento y la consecución de los objetivos propuestos por la Dirección.

Amenaza. Cualquier evento que, pueda provocar daños en los Sistemas de Información, produciendo a la empresa pérdidas materiales o financieras.

Vulnerabilidad. Cualquier debilidad en los Sistemas de Información y/o en el personal que administra el sistema, que pueda permitir a las amenazas causarles daño y producir pérdidas a la empresa.

Impacto. Es la medición (y valoración) del daño que podría producir a la empresa la materialización de una amenaza sobre los Sistemas de Información. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, que siempre será subjetiva, de los daños intangibles.

Riesgo. Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema de Información, causando un impacto en la empresa.

Defensa. Cualquier medio, físico o lógico, empleado para eliminar o reducir un riesgo. Debe realizarse una valoración cuantitativa de su coste.

3.2.2. Realización de Análisis de Riesgos

En el proceso de Análisis de riesgos se pueden diferenciar:

1. La Evaluación de Riesgos, orientada a determinar los Sistemas de Información que, en su conjunto o en cualquiera de sus partes, puedan verse afectados directa o indirectamente por amenazas, valorándose todos los riesgos y estableciendo sus distintos niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la empresa.
2. La Administración de Riesgos, que implica la identificación, selección, aprobación y manejo de las defensas (contra medidas) para eliminar, o reducir a niveles hyphenationaceptables aceptables, los riesgos evaluados, con actuaciones tendientes a: reducir la posibilidad de que una amenaza ocurra; limitar el impacto de una amenaza, si ésta se hyphenationmanifiesta manifiesta; reducir o eliminar una vulnerabilidad existente; permitir la recuperación del impacto o su transferencia a terceros (contratación de seguros) e incluye la aceptación del riesgo residual.

Es necesario actualizar periódicamente el análisis de riesgos tomando como base de partida el último realizado y las defensas implantadas hasta la fecha, por lo que los factores tiempo y medios necesarios para su realización serán menores.

El análisis de riesgos, además de centrarse en los Sistemas de Información existentes, es recomendable aplicarlo en el desarrollo de nuevos Sistemas, asegurándolos desde su creación.

3.3. Control

La actividad organiza y dirige el proceso de Administración de Seguridad de TI. Esta incluye la organización de la administración del marco de trabajo para la seguridad de la información. El marco de trabajo contiene la manera en la cuál será establecido el plan de seguridad, el proceso a través del cuál será implementado, y la manera en la cuál la implementación será evaluada, el proceso a través del cuál los resultados de esta evaluación serán usados para el mantenimiento del plan de seguridad y finalmente con ésta información se emitirá el reporte correspondiente para el cliente.

3.4. Plan

El primer paso en esta fase es la planeación, la investigación y la redacción de la norma. La creación de las normas implica identificar por qué se necesita (hyphenationrequerimientos requerimientos legales, regulaciones técnicas, contractuales u operacionales); determinar el alcance y la aplicabilidad de la norma, los roles y responsabilidades inherentes a la aplicación de la norma y garantizar la factibilidad de su implementación. La creación de una norma también incluye la investigación para determinar los requerimientos organizacionales para desarrollar las normas (es decir, que autoridades deben aprobarla, con quien se debe coordinar el desarrollo y estándares del formato de redacción), y la investigación de las mejores prácticas en la industria para su aplicación a las necesidades organizacionales actuales. De esta etapa se tendrá como resultado la documentación de la norma de acuerdo con los procedimientos y estándares de la organización, al igual que la coordinación con entidades internas y externas que la norma afectará, para obtener información y su aceptación.

Para propósitos de este proyecto de tesis la creación de las normas se desarrollan bajo los siguientes parámetros:

1. El estándar ISO/IEC-17799, debido a que define las mejores prácticas para gestionar la seguridad de la información.

2. El marco de trabajo de ITIL, define las mejores prácticas para asegurar la infraestructura de Tecnología de Información gestionada, y que se encuentra íntimamente relacionados con el uso de las mejores prácticas ISO/IEC-17799.

La actividad de Planeación se sustenta en una evaluación de riesgos de negocio para entender las amenazas y vulnerabilidades, y es requerida para moverse de una situación actual a la deseada.

El resultado deseado de esta fase es la determinación de las normas apropiadas basadas en el estándar ISO/IEC 17799 y el marco de trabajo de ITIL.

3.5. Evaluación

La revisión de la norma es una fase en el desarrollo del ciclo de vida. Una vez la documentación de la norma ha sido creada y la coordinación inicial ha sido empezada, esta debe ser remitida a un grupo (o un individuo) independiente para su evaluación antes de su aprobación final e implementación. Hay varios beneficios de la revisión independiente: una norma más viable a través del escrutinio de individuos que tienen una perspectiva diferente o más vasta que la persona que redactó la norma; apoyo más amplio para la norma a través de un incremento en el número de involucrados; aumento de credibilidad en la norma gracias a la información recibida de diferentes especialistas del grupo de revisión. Propio de esta etapa es la presentación de la norma a los revisores, ya sea de manera formal o informal, exponiendo cualquier punto que puede ser importante para la revisión, explicando su objetivo, el contexto y los beneficios potenciales de la norma y justificando porqué es necesaria. Como parte de esta función, se espera que el creador de la norma recopile los comentarios y recomendaciones para realizar cambios en la norma y efectuar todos los ajustes y las revisiones necesarias para obtener una versión final de la norma lista para la aprobación por los directivos.

Confiar ciegamente en las medidas de seguridad instaladas creará una atmósfera no segura. Una evaluación independiente habilita a otras partes de la organización a confiar en las medidas de seguridad, los resultados de la evaluación se usarán para mantener las medidas tomadas, es necesario mantener actualizadas las medidas para mayor eficiencia. La evaluación es indispensable para cerrar el ciclo del proceso de Administración de la Seguridad, cuando de la evaluación resulte necesario realizar un

cambio, este será submitido al proceso de Administración de Cambios por medio de un Petición de Cambio (RFC). Existen tres tipos de evaluaciones, las cuales son:

- Auditorías Internas, las cuales son revisiones desarrolladas por auditores de Procesamiento Electrónico de Datos (EDP, Electronic Data Processing)
- Auditorías Externas, las cuales son desarrolladas por auditores externos
- Evaluaciones propias, las cuales son desarrolladas por la propia organización

En el caso de este proyecto de investigación, esta fase se realizará mediante la *evaluación propia*, cabe mencionar que la evaluación toma lugar basándose en los incidentes de seguridad reportados.

3.6. Implementación

Incluye actividades relacionadas con la ejecución de la norma, asegurando que sea entendida por aquellos que requieren implementarla, monitorearla, darle seguimiento, reportar regularmente su cumplimiento y medir el impacto inmediato de la política en las actividades operativas. Dentro de estas actividades está la elaboración de informes a la administración de la implementación de la norma.

En ésta fase la actividad es implementar un rango completo de normas, las cuales limitaran los riesgos y las vulnerabilidades. Estas normas están basadas en en el estándar ISO/IEC-17799 y el marco de trabajo de ITIL y son clasificadas de acuerdo con el impacto que tengan en la información, la clasificación es la siguiente [5]:

1. *Preventivas*, son usadas para prevenir que ocurra un incidente de seguridad, y se pueden implementar mediante el control del uso de los derechos de acceso, autorizacion, identificación, autenticación y control de acceso a un grupo de personas. Un ejemplo de este tipo de norma es:
   - Verificar que el usuario tenga autorizacion del propietario del sistema para hacer uso del servicio o sistema de información. [13]
2. *Reductivas*, son aquellas que se deben realizar para minimizar los daños en caso de que ocurra un incidente. Un ejemplo de este tipo de norma es:
   - Desarrollar y probar una estrategia y programa de respaldo y recuperación [6].

3. *Represivas*, son medidas tomadas para actuar en caso de repetición de un incidente de seguridad. Por ejemplo, cuando una cuenta o dirección de red es bloqueada temporalmente después de numerosos intentos fallidos para logearse. Un ejemplo de este tipo de norma es:
   - Se deben de establecer procedimientos de monitoreo que registren intentos de acceso no autorizados, tales como:
     - Número de intentos de acceso fracasados
     - Violación a las políticas de acceso
     - Alertas de sistemas de detección de intrusos
4. *Correctivas*, son medidas tomadas cuando un daño debe ser reparado.Un ejemplo de este tipo de norma es:
   - Diseñar un plan de recuperación de acuerdo al proceso de manejo de incidentes [6].

3.7. Mantenimiento

La etapa de mantenimiento esta relacionada con el proceso de garantizar la vigencia y la integridad de la norma. Esto incluye hacer seguimiento a las tendencias de cambios (cambios en la tecnología, en los procesos, en las personas, en la organización, en el enfoque del negocio, etc) que puedan afectar la norma; recomendando y coordinando modificaciones resultado de estos cambios, documentándolos en la norma y registrando las actividades de cambio. Esta etapa también garantiza la disponibilidad continuada de la norma para todas las partes afectadas por ella, al igual que el mantenimiento de la integridad de la política a través de un control de versiones efectivo. Cuando se requieran cambios a la norma, las etapas realizadas antes deben ser revisadas.

Esta fase da paso la última fase del modelo que es un reporte, en el cual se llevará un registro histórico de los incidentes que ha experimentado la organización. Existen ventajas en tener una base de datos donde se documenten los incidentes de seguridad, lo cual permitirá realizar un análisis de tendencias en ciertos tipos de incidentes de seguridad, para ser capaces de proporcionar los argumentos y medidas necesarias requeridas.

3.7.1. Modelo de responsabilidad por etapa

La Tabla 3.1 proporciona una orientación para asignar responsabilidades a cada etapa de desarrollo del modelo de seguridad de TI, de acuerdo al nivel del requerimiento.

Etapa	**Responsable**
Planeación	Función Seguridad de Información
Implementación	Mandos medios y empleados involucrados
Evaluación	Cómite de Evaluación de Políticas
Mantenimiento	Función Seguridad Informática

Tabla 3.1: Modelo de Responsabilidades

La asignación de responsabilidades mostrada en la Tabla 3.1 se entiende mejor si se explora el modelo propuesto de acuerdo con las etapas del ciclo de vida.

Planeación. El departamento de Seguridad de Información debe ser quien proponga las políticas relacionadas con seguridad que engloban toda la organización y debe ser el responsable para crear tanto las políticas, normas, estándares, mejores prácticas, y guías.

Implementación. Los mandos medios y empleados para quienes las políticas de seguridad son aplicables son los principales involucrados en la implementación y garantía inicial del cumplimiento de políticas que hayan sido públicadas recientemente.

Evaluación. El establecimiento de un comité de evaluación de políticas proporciona un foro de amplio espectro para revisar y evaluar la viabilidad de las políticas, normas, estándares, mejores prácticas, y guías que afecten a toda la organización. Aquí se propone que esta labor sea realizada por los comités de informática, que en un principio están conformados por personas de diversas áreas organizacionales, interesadas en la seguridad informática. La responsabilidad del comité es revisar que las normas estén bien redactadas, sean comprensibles, estén coordinadas y sean viables en términos de las personas y tecnologías que afecta.

Mantenimiento. Debido a su responsabilidad en el programa de seguridad de información de la organización, el departamento de seguridad de información es el que mejor está posicionado para dar mantenimiento a las normas de seguridad que tengan aplicabilidad en toda la organización para garantizar que estén actualizadas y disponibles a todos los afectados.

3.8. Método de Investigación

3.8.1. Tipo de Investigación

El tipo de investigación seguida en este proyecto de tesis, es la documental, debido a que este método según [9] se centra exclusivamente en la recopilación de datos existentes en forma documental, ya sea de libros, textos u otros tipos de documentos, en el caso de este proyecto la recopilación de información para la creación de normas es del estándar ISO/IEC-17799 e ITIL, debido a su importancia en el área de Tecnología de Información. En esta investigación se obtienen antecedentes para profundizar en las teorías y aportaciones, ya emitidas sobre el tópico que es objeto de estudio, se complementa y deriva nuevo conocimiento, a fin de enriquecer lo ya existente.

3.8.2. Etapas de la investigación

La Figura 3.2, muestra las fases que se llevan acabo como parte de la metodología de investigación, para la creación de las normas de seguridad para los procedimientos de seguridad de información para la empresa Alestra.

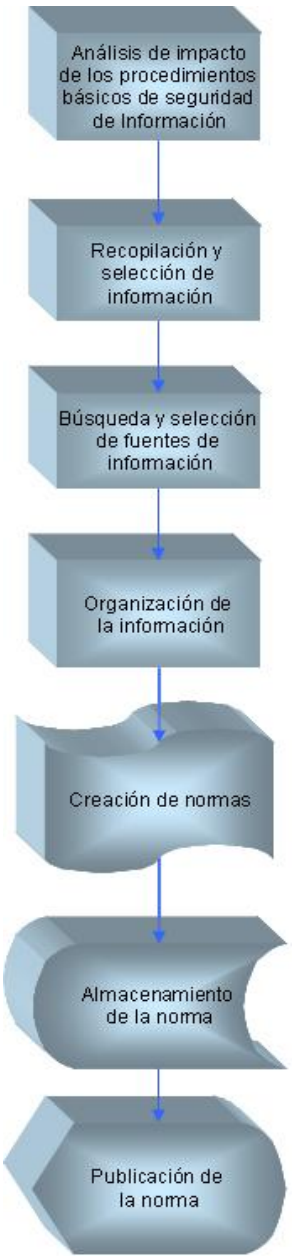


Figura 3.2: Diagrama de Fases de Investigación

1. **Análisis de impacto de los procedimientos básicos de seguridad de Información.**
   Para realizar normas adecuadas de seguridad de información para los procedimientos de seguridad de información de interés por parte de la empresa Alestra es necesario medir el impacto que estos producen en el entorno empresarial (lo cual se llevó a cabo en la etapa de análisis de riesgos por parte del equipo del

área de seguridad de información de Alestra) y que será vital para reevaluar procedimientos y normas, a fin de conocer cómo influyen los procedimientos básicos en el comportamiento organizacional.

Dentro del estudio de impacto de procedimientos básicos de seguridad de información se identifican las siguientes variables:

- *Independientes*: Procedimientos de seguridad de información determinados por la empresa Alestra, controles sugeridos por el estándar ISO/IEC-17799 y mejores prácticas establecidas por el ITIL, para el establecimiento de mecanismos adecuados a fin de lograr un nivel confiable de seguridad.

- *Dependientes:* Implementación de normas para garantizar un mayor grado de seguridad de información, proceso de evaluación e implantación adecuado, cuenta con todos los factores, recomendaciones y sugerencias, evaluaciones de expertos y/o profesionales en el área de seguridad de la información y en la implementación del estándar ISO/IEC-17799, haciendo de esta manera que la implementación de las normas de seguridad descritas en este trabajo de tesis, garanticen niveles altos de confidencialidad, integridad y disponibilidad de la información de la empresa Alestra.

2. **Recopilación y selección de información.**

En esta fase de la investigación se identifica la información pertinente y relevante para la empresa. La fase de recopilación de información se basa directamente en el Análisis de Riesgos, en el cuál se observa la probabilidad de que una amenaza haga uso de una vulnerabilidad potencial particular y el impacto resultante de este evento.En el análisis de riesgos se tomó en cuenta lo siguiente:

a) Identificación y Clasificación de Activos
b) Identificación y Determinación de Amenazas
c) Identificación y Determinación de vulnerabilidades
d) Medición de Impacto
e) Determinación de riesgo

Como resultado del análisis de riesgos, se identificó que los procedimientos básicos de seguridad de información que tienen mayor impacto a la Confidencialidad, Integridad y Disponibilidad de la información son los siguientes:

a) Respaldo de Información

b) Registro Usuarios y Administración de Privilegios
c) Controles contra Software Malicioso
d) Monitoreo y Registro de eventos

Por lo cual los anteriores procedimientos se deben tomar en cuenta para la creación de las normas de seguridad de información.

3. **Búsqueda y selección de fuentes de información.**

   De acuerdo a la información de la fase anterior de la investigación, se determinó que las siguientes fuentes de información para la creación de normas de seguridad para los procedimientos básico de seguridad de información, son las adecuadas debido a su importancia en el área de seguridad de TI:

   a) Para el establecimiento del modelo de seguridad de información la principal fuente es es el libro de ITIL, *Best Practice for Security Management. ITIL. The key to Managing IT Service.*

   b) Para el establecimiento de las normas de seguridad, se toma como fuente de información el estándar ISO/IEC-17799 y los diferentes libros de ITIL en los que se destacan:
      - Best Practice for Security Management. ITIL. The key to Managing IT Service.
      - Best Practice for ICT Infrastructure Management. ITIL The key to Managing IT services.
      - Best Practice for Service Support. ITIL. The key to Managing IT Service.
      - Best Practice for Delivery Support. ITIL. The key to Managing IT Service.

4. **Organización de la información.**
   Un elemento clave en la gestión del conocimiento es una correcta organización de la información, debido a que ambas actividades se encuentran estrechamente relacionadas. El conocimiento se construye a partir de la información recibida, y esta última se manifiesta como conocimiento explícito en el entorno empresarial mediante disímiles formas, tales como: mensajes, informes, circulares, manuales de procedimiento o normas, como es el caso de este proyecto de tesis, por lo cual, Los sistemas de gestión documental son por lo tanto fundamentales.

El producto resultante de este análisis de la información es la creación de las normas de seguridad para los diferentes procedimientos básicos de seguridad de información determinados por la empresa Alestra, las cuales deben presentarse en un lenguaje sencillo, legible, exhaustivo, coherente, directo, sin ambigüedades y con un orden lógico que resista cualquier crítica o duda, especificar claramente lo que se quiere dar a entender. Debe ser, además, veraz y profundo, adaptarse a necesidades de los usuarios a quienes se dirige, considerar el contexto en que se realiza y los objetivos funcionales que se persiguen con estas normas.

5. **Creación formal de documentos de normas.**

El resultado de la organización de la información para los procedimientos básicos de seguridad de información, es presentado en manera de normas, las cuales siguen un formato especifico (ver sección 4.1.1), el cual ayuda al lector a entenderla, los puntos importantes que conforman el formato de la norma son los siguientes:

a) **Título de la norma**. Se refiere al procedimiento básico de seguridad de información, para el cuál se desarrolla la norma.

b) **Nombre de quien la elaboró.** Se refiere a la persona responsable de la creación de la norma.

c) **Nombre de quien la aprueba.** Se refiere a la persona quien evalúa y aprueba el contenido de la norma, el cual debe ser un experto en el área. El objetivo de este punto es obtener el apoyo necesario, a través de la firma de una persona ubicada en una posición de autoridad. La aprobación permite iniciar la implementación.

d) **Identificación de la norma.** Se refiere a la nomenclatura que se le asigna a la norma, para facilitar su uso dentro de la empresa.

e) **Fecha de elaboración.** Se refiere a la fecha de creación de la norma.

f) **Fecha de implementación**. Se refiere a la fecha en la cual se implementará de manera práctica la norma, dentro de la empresa.

g) **Fecha de revisión.** Se refiere a la fecha en la cual se debe revisar la norma con el objetivo de actualizarla en caso necesario.

6. **Almacenamiento de la Información.**

   En cuanto al almacenamiento y recuperación, se propone crear una intranet coherente y útil para la empresa, que contemple el sistema de gestión documental, lo cual es un punto esencial en la actividad del especialista en información a la hora de organizar la información y es clave para el éxito del proyecto. La tarea consiste en concebir una visión integradora de la información, que comprenda la totalidad de los documentos de las normas, de tal manera que estén disponibles para quienes requieran consultarlas o hacer uso de las mismas.

7. **Diseminación de la Información.**

   La comunicación de las normas es una fase muy importante y necesaria para la implementación de las mismas, las normas deben ser inicialmente difundida a los miembros que sean afectados directamente por la norma, esta fase implica determinar el alcance y método inicial de distribución de la norma, es posible que deban tomarse en cuenta factores como; ubicación geografica y línea de mando que será utilizada para comunicar la norma. Esta fase debe planearse con el fin de determinar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de la norma, por parte a quien va diriguida.

Capítulo 4

Creación de Normas Basadas en ITIL e ISO/IEC-17799

4.1. Respaldo de Información

No es ninguna novedad el valor que tiene la información y los datos para una empresa. Lo que resulta increíble de esto es la falta de precauciones que se suela tener al confiar plenamente en el sistema de almacenamiento.
Cuando la información se ve amenazada frente un incidente de seguridad, el daño puede ser irreversible, puede significar la pérdida total de la información. Es principalmente por esta razón, por la que debemos respaldar la información importante. Si esto llega a suceder a una empresa, las pérdidas económicas pueden ser cuantiosas sino existe un mecanismo de recuperación. Los negocios de todos los tipos y tamaños confían en la información computarizada para facilitar su operación.
La tecnología no está exenta de fallas o errores, y los respaldos de información son utilizados como un plan de contingencia en caso de que una falla o error se presente.
Asimismo, hay empresas, que por la naturaleza del sector en el que operan (por ejemplo Banca) no pueden permitirse la más mínima interrupción informática.
Según [11] interrupciones se presentan de formas muy variadas: virus informáticos, fallos de electricidad, fallas de hardware y software, caídas de red, hackers, errores humanos, incendios, inundaciones, etc. Y aunque no se pueda mitigar cada una de estas interrupciones, la empresa sí puede prepararse para evitar las consecuencias que éstas puedan tener sobre su negocio. Del tiempo que tarde en reaccionar una empresa dependerá la gravedad de sus consecuencias. La Figura 4.1, muestra los riesgos en los cuales se encuentran inmersos los sistemas de información, los mismos que deben ser considerados para estar conscientes de la importancia de respaldar la información de la empresa de manera oportuna.

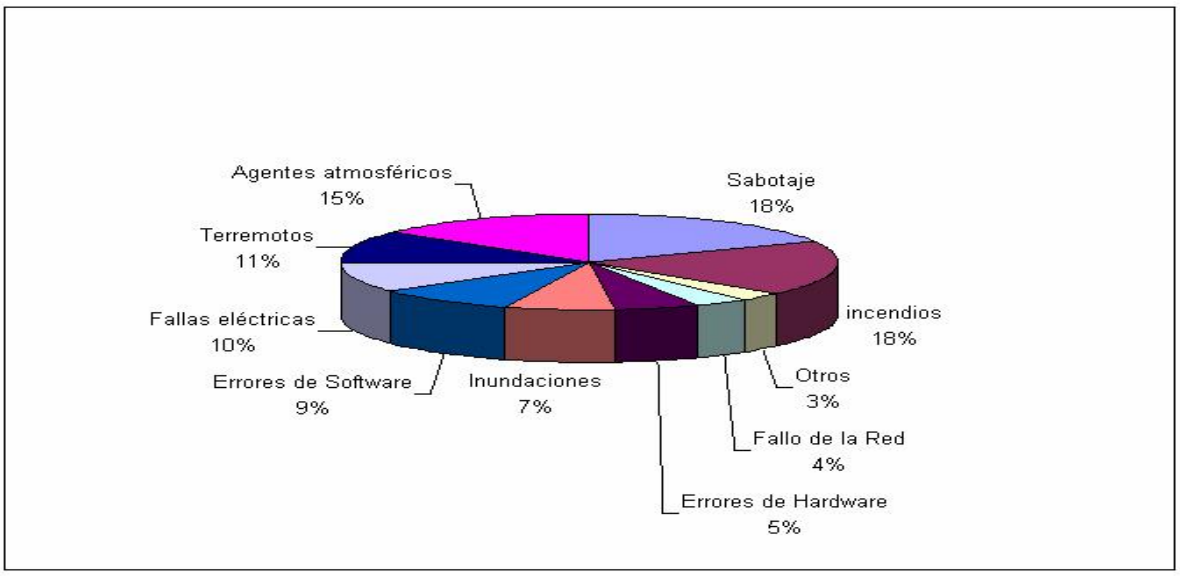


Figura 4.1: (IBM, 2003) Riesgos a los cuales se enfrentan los sistemas de información

Clasificación de los respaldos

Copias de Información. Estos respaldos son sólo duplicados de archivos que se guardan en medios magnéticos de alta capacidad. Los archivos que son respaldados pueden variar desde archivos del sistema operativo, bases de datos, hasta archivos de un usuario común. Existen varios tipos de Software que automatizan la ejecución de estos respaldos, pero el funcionamiento básico de estos paquetes depende del denominado archive bit . Este archive bit indica un punto de respaldo y puede existir por archivo o al nivel de "Bloque de Información", esto dependerá tanto del software que sea utilizado para los respaldos así como el archivo que sea respaldado. Este mismo archive bit es activado en los archivos (o bloques) cada vez que estos sean modificados y es mediante este bit que se llevan acabo los tres tipos de respaldos comúnmente utilizados [2]:

1. Respaldo Completo: Guarda todos los archivos que sean especificados al tiempo de ejecutarse el respaldo. El archive bit es eliminado de todos los archivos (o bloques), indicando que todos los archivos ya han sido.
2. Respaldo de Incremento: Cuando se lleva acabo este tipo de respaldo, sólo aquellos archivos que tengan el archive bit serán respaldados; estos archivos (o bloques) son los que han sido modificados después de un respaldo completo. Además cada

respaldo de incremento que se lleve acabo también eliminará el archive bit de estos archivos (o bloques) respaldados.

3. Respaldo Diferencial: Este respaldo es muy similar al "Respaldo de Incremento", la diferencia estriba en que el archive bit permanece intacto.

En la Tabla 4.1, se puede visualizar las características de los respaldo de información:

Respaldo	**Archivos en respaldo**	**Archive bit**	**Ventajas**	**Desventajas**
Completo	Todos	Eliminado en todos los archivos	Con este respaldo es posible recuperar toda la información	Tiempo de Ejecución
De incremento	Archivos con archive bit activo (Aquellos que hayan cambiando desde el último respaldo completo)	Eliminado en los archivos que se respaldan	Velocidad	Requiere del último respaldo y de todos los respaldos de incremento que le siguieron para recuperar el sistema
Diferencial	Archivos con archive bit activo (Aquellos que hayan cambiando desde el último respaldo completo)	Intacto	Requiere el último respaldo completo y el último respaldo diferencial	Ocupa mayor espacio en discos comparado con respaldo de incremento

Tabla 4.1: Clasificación de Respaldos

4.1.1. Norma para el Respaldo de Información

ALESTRA	Respaldo de Información
Elaborado por: Rubí Shelby Jaramillo Islas	**Identificación:** AN-SA-SI-05
	Fecha de Elaboración: 16 Noviembre 2004
Aprobado por: Ricardo Morales González	**Fecha de Implementación:** 1 Enero 2005
	Fecha de Revisión: 1 Junio 2005

Explicación:

El respaldo y recuperación de información son complementarios en el sentido que el respaldo es casi siempre programado y la recuperación es usualmente una actividad reactiva y no es programada. Esto significa que el procedimiento de respaldo de información raramente necesita ser realizado de manera presionada mientras que el procedimiento de recuperación de información es hecho por razones de restauración de información. El procedimiento de respaldo es parte del proceso de Manejo de Seguridad y de Disponibilidad, que garantiza la duplicación de datos para la recuperación de los mismos en circunstancias anormales o para archivar la información durante un largo periodo, el cual es especificado por la política de retención. La recuperación es el elemento del manejo de Seguridad y Disponibilidad que garantiza la restauración exitosa de los datos previamente respaldados [14].

1. **Objetivo:**
   Este elemento de operación es el responsable del control y el manejo de todos los aspectos de almacenamiento y recuperación de información e incluye todos los procesos y mecanismos necesarios para asegurar que niveles apropiados de almacenamiento, protección, acceso y recuperación de datos estén disponibles y sean usados en el momento necesario.

2. **Aplicación:**
   Este documento tiene como audiencia todo aquel personal de la empresa que directa o indirectamente este involucrado en la operación, manipulación, procesamiento y almacenamiento de información de negocios, empleados y clientes de la empresa; generada por los productos y servicios ofrecidos por la empresa, los sistemas administrativos y la infraestructura de comunicación.

3. **Directrices:**
   Se deben considerar los siguientes controles:
   a) Deben ser hechas regularmente copias de respaldo de información esencial del negocio y del software [14].
   b) Se deben proporcionar instalaciones apropiadas para asegurar que la información esencial del negocio y del software puede ser recuperada en caso de desastre o falla [14].
   c) Los arreglos de respaldo de sistemas individuales deben ser probadas regularmente para asegurar que ellos conocen los requerimientos de continuidad de negocio [14].
   d) Se debe mantener un nivel mínimo de información de respaldo, junto con un registro exacto y completo de las copias de respaldo y procedimientos de restauración documentados, los cuales se deberán almacenar en un lugar remoto, a suficiente distancia para escapar de algún daño en caso de desastre en el sitio principal. Se deben retener al menos las últimas 3 generaciones o ciclos o respaldo de información de aplicaciones importantes para el negocio [13].
   e) Se le debe proporcionar un nivel adecuado de protección física a la información de respaldo, que sea consistente con los estándares aplicados al sitio principal. Los controles aplicados al medio del sitio principal deben ser extendidos para cubrir el sitio de respaldo [13].
   f) El medio de respaldo debe ser probado regularmente, para asegurar que se puede confiar en ellos en caso de emergencia [13].
   g) Se deben probar regularmente los procedimientos de restauración, para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en un procedimiento operacional de recuperación [13].

h) Asegurarse que existen procedimientos operacionales de respaldo y recuperación y que estos cumplen con las políticas de respaldo y recuperación [14].

i) Especificar, seleccionar y administrar el uso de herramientas y paquetes de respaldo y recuperación de datos [14].

j) Especificar, seleccionar y administrar el uso de paquetes operacionales de soporte, ej. manejo de discos, cintas [14].

k) Ordenar cintas magnéticas, disquete, cartuchos, papel y otros medios o dispositivos cuando sean necesarios.

l) Desarrollar y mantener sistemas de logs para registrar el uso de todos los medios de ICT (Information Communication Technology), para asegurar un adecuado nivel de respaldo [14].

m) Configurar y mantener un sistema de identificación física para cintas magnéticas, cartuchos, etc., para una fácil identificación [14].

n) Desarrollar respaldos seguros y rotación asociada de medios, asegurando que las cintas de respaldo están en un ambiente seguro [14].

ñ) Determinar los requerimientos de respaldo y recuperación, los cuales deben cubrir hardware y software [6].

o) Desarrollar y probar una estrategia y programa de respaldo y recuperación [6].

p) Diseñar un plan de recuperación de acuerdo al proceso de manejo de incidentes [6].

4. **Referencias:**

[**6**]. Office Governmet Commerce. *Best Practice for Service Support. ITIL. The key to Managing IT Service.* 1era edición, 2002.

[**13**]. British Standard Institute. *British Standard ISO/IEC 17799-1.* 2da edición, 2003.

[**14**]. British Standard Institute. *British Standard BS 7799-2.* 2da edición, 2003.

4.2. Registro de Usuarios y Administración de Privilegios

El control de usuarios es una actividad crítica para el responsable de la administración de los recursos del sistema, la administración de usuarios requiere saber como establecer contraseñas y permisos de acceso a la información.

La seguridad de la información y por consiguiente de los equipos informáticos, es una cuestión que llega a afectar, incluso, a la vida privada de la persona humana, de ahí que resulte obvio el interés creciente que día a día se evidencia sobre este aspecto de la nueva sociedad informática.

Ladrones, manipuladores, saboteadores, espías, etc. reconocen que el centro de cómputo de una institución es su nervio central, que normalmente tiene información confidencial y que, a menudo, es vulnerable a cualquier ataque.

La seguridad de la información tiene dos aspectos. El primero consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar protección de la "privacidad", si se trata de datos personales, y mantenimiento de la seguridad en el caso de datos institucionales.

Un segundo aspecto de la protección es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado [1].

En general, la protección de los datos requiere ejercer un control sobre la lectura, escritura y empleo de esa información. Para obtener mayor eficiencia en la protección se debe tener siempre presente la protección de los datos, el mantenimiento de la privacidad y la seguridad del secreto.

El secreto se logra cuando no existe acceso a todos los datos sin autorización. La privacidad adecuada puede lograrse cuando los datos que puedan obtenerse no pueden enlazarse a individuos específicos o no pueden utilizarse para imputar hechos acerca de ellos.

Según [10], la falta de medidas adecuadas de seguridad puede ocasionar accesos no autorizados a:

- Area de Sistemas.
- Computadoras personales y/o Terminales de la red.
- Información Confidencial.

Algunos usuarios o extraños (personal no autorizado) pueden encontrar alguna forma mediante la cual, logren el acceso al sistema o la base de datos y descubrir información clasificada o datos no autorizados. Por lo que según [10] se deben considerar medidas de seguridad tales como:

Programas de Control. Son programas protegidos que mantienen y controlan a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente. El uso de tal programa puede conferir al usuario algunos de los privilegios que corresponden al controlador de dichos programas. La transferencia de privilegios es adecuada si el programa actúa como filtro de la información.

Establecer Contraseñas. La "contraseña" es una palabra especial o código que debe teclearse al sistema de computadora antes que se realice un proceso. Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados.

La identificación de un individuo debe ser muy difícil de imitar y copiar. Aunque su nombre pueda ser único, es fácil que cualquiera que observe a quienes tienen acceso al sistema lo copie, por lo que no es una clave adecuada.

Una vez que se obtiene una clave de acceso al sistema, ésta se utiliza para entrar al sistema de la base de datos desde el sistema operativo. La responsabilidad del manejo de la clave corresponde tanto al que accesa como al sistema operativo.

A fin de proteger el proceso de obtención de una llave del sistema, cuando el usuario realiza la entrada (en inglés LOGIN), solicita una clave de acceso con el nombre del usuario, la cual consiste de unas cuantas letras elegidas por el usuario.

Establecer nivel de acceso (privilegios). Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas. De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

1. Nivel de consulta de la información no restringida o reservada.
2. Nivel de mantenimiento de la información no restringida o reservada.
3. Nivel de consulta de la información incluyendo la restringida o reservada.
4. Nivel de mantenimiento de la información incluyendo la restringida.

4.2.1. Norma para el Registro de Usuarios y Administración de Privilegios

ALESTRA	**Registro de Usuarios y Administración de Privilegios**
Elaborado por: Rubí Shelby Jaramillo Islas	**Identificación:** AN-SA-SI-11
	Fecha de Elaboración: 16 Noviembre 2004
Aprobado por: Ricardo Morales González	**Fecha de Implementación:** 1 Enero 2005
	Fecha de Revisión: 1 Junio 2005

Explicación:

Se deben establecer procedimientos formales para controlar la localización de derechos de acceso a los sistemas y servicios de Información. Los procedimientos deben cubrir todas las etapas del ciclo de vida de acceso a los usuarios, desde el registro inicial de nuevos usuarios hasta el registro final de los usuarios. Se debe poner especial atención, a la necesidad de controles para el almacenamiento de derechos de acceso privilegiados, lo cual permite a los usuarios anular los controles en el sistema [13]. Se debe controlar el acceso a servicios de información multiusuario a través de un procedimiento formal de registro.

1. **Objetivo:**
   Este proceso se refiere a prevenir el control de acceso a la información y a los sistemas de información, para proteger la confidencialidad de la información y prevenir cambios no deseados y no autorizados, daños, destrucción de la información o software, y para prevenir interrupciones en el proceso normal de producción. Se hace la diferencia entre seguridad de acceso en relación a redes, equipo de computo y aplicaciones. Se deben establecer procedimientos formales para el registro de usuarios para conceder acceso a multiusuarios a sistemas y servicios de información.

2. **Aplicación:**
   Este anexo tiene como audiencia a todos los usuarios, administradores de sistemas y redes, Gerentes y Responsables de Áreas de la empresa.

3. **Directrices:**
   Los controles son los siguientes:

   a) El usuario debe hacer uso de un identificador único, con el cuál que pueda ser relacionado y hacerlo responsable de sus acciones. El uso de identificadores de grupo solo serán permitidos cuando sea conveniente para el trabajo realizado. [13]
   b) Verificar que el usuario tenga autorización del propietario del sistema para hacer uso del servicio o sistema de información. [13]
   c) Verificar que el nivel de acceso concedido es apropiado para el propósito del negocio y que sea consistente con la política de seguridad de la organización. [13]
   d) Proporcionar a los usuarios un documento escrito en el cuál se indiquen sus derechos. [13]
   e) Pedir que los usuarios que firmen un documento donde se indique que entienden las condiciones de los derechos de acceso. [13]
   f) Asegurar que al proveedor de servicios no se le proporcione acceso. [13] hasta que sean completados los procedimientos de autorización
   g) Mantener un registro formal de todas las personas registradas con derecho a usar los servicios. [13]
   h) Remover inmediatamente los derechos de acceso de los usuarios quienes hayan cambiado de área de trabajo o abandonado la organización. [13]
   i) Verificar periódicamente las cuentas de los usuarios y remover aquellos identificadores de usuarios que resulten redundantes
   j) Asegurar que los identificadores redundantes de usuarios no son usados por otros usuarios. [13]
   k) Mantener un control efectivo sobre los derechos de acceso: Asegurarse que se mantengan controles de acceso efectivos y que incluyan la administración de cuentas de usuario, derechos, así como la autenticación de los mismos (incluyendo passwords y tokens) que permita el acceso a derechos actualizados.[5]
   l) Las responsabilidades de los usuarios finales, son de acuerdo, la responsabilidad de la organización del cliente. Esto hace que la organización del cliente diriga sus responsabilidades mas explícitamente en los SLAs, un plan de seguridad efectivo depende de la cooperación de los usuarios, en este

punto es esencial la concientización. Se debe poner atención especifica a las responsabilidades de los usuarios en los siguientes subpuntos [5]:

1) Uso de contraseñas
   - Cada usuario individual deberá tener su propia cuenta y contraseña y mantenerlas en secreto de manera responsable.[13], [5]
   - Evitar que el password permanezca registrado en papel, solo quedará registrado en papel cuando sea necesario por alguna razón de emergencia, mantener este papel en un sobre sellado y almacenarlo en un lugar seguro,para asegurar que la contraseña será usada solamente por la persona autorizada siguiendo los procedimientos apropiados de caso de emergencia. [13], [5]
   - Cambiar la contraseña en intervalos periódicos, se recomienda que se haga cada mes. [13], [5]
   - La longitud mínima de las contraseñas debe ser de 6 caracteres, se deberá seleccionar una contraseña que incluya caracteres numéricos, alfabéticos y especiales. [13], [5]
   - Evitar el uso de contraseñas temporales, al menos que sea absolutamente necesario pero en caso de ser usado, cambiarlo en el primer Login. [13], [5]
2) No abandonar sesión activas, equipos y datos en estado activo
   - El usuario debe log off (deslogearse) cuando abandone el equipo por algún periodo. [13], [5]
   - En este caso, exhortar al uso de protectores de pantalla automáticos y bloqueadores de teclado. [13], [5]
   - Los usuarios deben tomar precauciones específicas con equipos, tales como, laptops, cuando se usen en circunstancias inseguras, por ejemplo en situaciones donde el equipo pueda ser robado, en este caso los candados físicos pueden ser útiles. [13], [5]
3) No desatender procedimientos de importación y exportación de software y de datos
   - Los usuarios tienen la responsabilidad de la detección y prevención de virus. Los usuarios finales que importen información deberán verificar que se encuentre libre de virus. [13], [5]
   - No debe se importar software por parte de los usuarios, en caso de ser así, se hará a través de un canal apropiado y seguro. [13], [5]

- En caso de que los usuarios importen y exporten datos, los procedimientos de respaldo no podrán ser completamente controlados por el proveedor de servicios, y los usuarios asumirán la responsabilidad. [13], [5]
- Concientizar a los usuarios acerca de los riesgos específicos que pueden ocurrir cuando se trabaja remotamente. [13], [5]

4) Uso de fuentes externas
   - Concientizar a los usuarios del uso correcto de Internet. [13], [5]
   - Aplicar los mismo para el uso de correo electrónico y otras formas de intercambio de datos de manera electrónica. [13], [5]
   - No permitir que se abran facilidades de comunicación de datos por acceso remoto. [13], [5]
   - El acceso remoto solo deberá ser posible a través de canales autorizados. [13], [5]
   - No se debe usar software proveniente de Internet. [13], [5]
   - El usuario debe ser conciente de que las facilidades son proporcionadas solamente para propósitos de negocio. [13], [5]

5) Manejo de Incidentes
   - Reportar el incidente de seguridad tan pronto como sea posible a través de un canal directo al proceso de Control de Incidentes / Help Desk, a través del cuál tomará lugar el manejo del incidente. [13], [5]

4. **Referencias:**

[**5**]. Office Government Commerce. *Best Practice for Security Management. ITIL. The key to Mananing IT Service.* 1era edition, 2000.

[**13**]. British Standard Institute. *British Standard ISO/IEC 17799-1.* 2da edición, 2003.

4.3. Controles contra software malicioso

Código malicioso se refiere a cualquier programa o código malicioso o no esperado como son virus, troyanos y droppers. No todos los programas maliciosos o códigos son virus. Los virus sin embargo, ocupan la mayoría de todo el código malicioso conocido a la fecha, incluyendo gusanos. Los otros principales tipos de código malicioso son Troyanos, droppers y kits.

Debido a las múltiples facetas de un código malicioso o de un programa malicioso, el referirlo como código malicioso ayuda a evitar la confusión. Por ejemplo, un virus que además cuenta con características tipo Troyano puede ser llamado código malicioso.

Un troyano es un código malicioso que realiza acciones no esperadas o no autorizadas, normalmente maliciosas. La principal diferencia entre un troyano y un virus es la inhabilidad para replicarse. Los Troyanos causan daño, comportamiento inesperado del sistema y comprometen la seguridad de los sistemas, pero no se replican. Si este se replica entonces se debe de clasificar como un virus.

Un Troyano, tomado de la mitología griega del Caballo de Troya, típicamente viene en un correcto empaquetamiento, pero tiene intenciones ocultas dentro de su código. Cuando un troyano es ejecutado, los usuarios experimentarán problemas inesperados en la operación del sistema, y en algunos casos pérdida de datos valiosos. Según un reporte emitido por Symantec [15], mas de 994 nuevos virus y gusanos de Win32 fueron documentados en la primer mitad de 2003, mas del doble de los 445 documentados en la primer mitad de 2002.

A medida que aumenta el uso de clientes de mensajería instantánea y networking cliente a cliente, nuevos gusanos y virus utilizan estos mecanismos para propagarse. De las 50 principales emisiones de código malicioso documentadas en la primer mitad de 2003, 19 utilizaba aplicaciones cliente a cliente y mensajería instantánea un aumento de casi el 400 por ciento en solo un año.

Las emisiones de código malicioso con puertas traseras ha aumentado casi un 50 por ciento, aumentando de 11 a 17 emisiones en la primer mitad de 2003. El intento mas visible de robo de datos confidenciales fue el lanzamiento de Bugbear.B en junio

de 2003. El descubrimiento de este variante aumento seriamente la preocupación ya que su objetivo específico eran las instituciones bancarias.

4.3.1. Norma contra software malicioso

ALESTRA	**Control contra Software Malicioso**
Elaborado por: Rubí Shelby Jaramillo Islas	**Identificación:** AN-SA-SI-06
	Fecha de Elaboración: 16 Noviembre 2004
Aprobado por: Ricardo Morales González	**Fecha de Implementación:** 1 Enero 2005
	Fecha de Revisión: 1 Junio 2005

1. **Objetivo:**
   Este elemento operacional se refiere a implementar controles y procedimientos para proteger de software malicioso. La protección debe ser basada en la concientización de la seguridad de la información, acceso apropiado a los sistemas y controles de administración de cambios.

2. **Aplicación:**
   Este anexo tiene como audiencia todo aquel empleado de la empresa, así como al personal subcontratado, prácticantes y cualquier otras terceras partes relacionadas que tengan acceso a los recursos de cómputo de la compañía.

3. **Directrices:**
   Deben ser considerados los siguientes controles:
   a) Cumplir formalmente con licencias de software y prohibir el uso de software no autorizado [13].
   b) Política formal para proteger de riesgos asociados con la obtención de archivos y software vía redes externas, o algún otro medio, la cual indique las medidas de protección que deberán ser tomadas [13].
   c) Instalación y actualización de software de detección de virus, el cual escanee las computadoras como rutina básica [13].
   d) Realizar revisiones de manera regular del software y datos contenidos en sistemas que soportan los procesos de negocio críticos [13].
   e) La presencia de archivos desaprobados o no autorizados deben ser formalmente investigados [13].

f) Verificar archivos de medios electrónicos de origen incierto o no autorizado, o archivos recibidos de redes no confiables [13].

g) Manejar procedimientos y responsabilidades para tratar con un posible ataque de virus en los sistemas, tener procedimientos de entrenamiento de usuarios,de reporte y recuperación de ataques de virus [13].

h) Tener un plan de continuidad de negocios para el respaldo y recuperación de datos y software necesario en caso de ataque de virus [13].

i) Se deben tener procedimientos para verificar toda información relacionada a software malicioso, con el fin de asegurar que los boletines de advertencia son exactos e informativos [13].

j) Los administradores deben asegurarse que provienen de fuentes calificadas, p. e. sitios de Internet confiables, proveedores de software de antivirus o revistas formales, con el fin de diferenciar una falsa alarma de un virus real [13].

k) El staff debe ser consiente de las falsas alarmas y saber actuar en caso de recibirlas [13].

l) Apagar y remover servicios innecesarios [15].

m) Mantener actualizados los niveles de parches, especialmente en computadoras que mantienen servicios públicos y que son accesibles a través del firewall, tales como servicios HTTP, FTP, mail, y DNS

n) Reforzar una política de passwords [15].

ñ) Configurar los servidores de correo electrónico para bloquear o remover correos que contengan adjuntos comúnmente usados para propagar virus, tales como .vbs, .bat, .exe, .pif y .scr [15].

o) Aislar las computadoras infectadas rápidamente para prevenir que se comprometa toda la organización [15].

p) Realizar un análisis forense y restaurar las computadoras usando un medio confiable [15].

q) Entrenar a los empleados para que no abran adjuntos a menos que los estén esperando. Y a no ejecutar software que haya sido descargo de Internet a menos que haya sido previamente escaneado de virus [15].

r) Garantizar que se cumplan los procedimientos de respuesta ante emergencias. Probar la seguridad para garantizar que se lleven a cabo los controles adecuados [15].

4. **Referencias:**

[**13**]. British Standard Institute. *British Standard ISO17799-1*. 2da edition, 2003.

[**15**]. Symantec. *Aumento en las amenazas combinadas, vulnerabilidades y ataques en internet*. www.symantec.com, Octubre 2003.

4.4. Monitoreo y Registro de Eventos

El monitoreo de redes tiene como principal objetivo recolectar información útil a cerca del funcionamiento de la red, y utilizarla para detectar tendencias y planear un mejor desempeño de la misma. También permite reducir cuellos de botella optimizando el servicio, detectar fallas para recuperar al sistema de crisis y realizar diagnósticos que permitan lograr arreglos antes de que los usuarios finales vean mensajes de error e incrementar la disponibilidad y utilización del sistema teniendo en cuenta cuestiones de seguridad.

El monitoreo de redes es necesario en ambientes distribuidos, ya que existen cuentas críticas para el funcionamiento de la red, así como para advertir las necesidades de crecimiento y ser capaces de administrar redes complejas y reducir los recursos necesarios para el funcionamiento de la misma. Se deben cumplir con tres áreas fundamentales del monitoreo de redes: el monitoreo de prestaciones, el monitoreo de fallas y el monitoreo de contabilidad.

La gestión de prestaciones evalúa el comportamiento de la red y para ello utiliza indicadores como los siguientes:

- Disponibilidad: Tiempo que un componente está disponible para los usuarios
- Factor de bloqueo: La cantidad de usuarios que en teoría no pueden acceder a la red por encontrar ocupada la señal
- Tiempo de respuesta: Tiempo transcurrido hasta que se recibe la respuesta de un dispositivo de la red
- Exactitud: Cantidad de paquetes defectuosos en la red en un determinado período de tiempo
- Throughput: Número de paquetes que viajan en la red en un determinado período de tiempo

ALESTRA	Monitoreo y Registro de Eventos
Elaborado por: Rubí Shelby Jaramillo Islas	**Identificación:** AN-SA-SI-03
	Fecha de Elaboración: 16 Noviembre 2004
Aprobado por: Ricardo Morales González	**Fecha de Implementación:** 1 Enero 2005
	Fecha de Revisión: 1 Junio 2005

4.4.1. Norma para Monitoreo y Registro de Eventos

Explicación:

Monitorear los sistemas permite que sea verificada la efectividad de los controles adoptados conforme al modelo de la política de acceso.

1. **Objetivo:**
   Registrar y detectar actividades no autorizadas en elementos informáticos y en redes de la empresa. Los sistemas y redes deben ser monitoreados para detectar desviaciones en las políticas de control de acceso y registrar los eventos correspondientes con el fin de proveer evidencia en caso de ocurrir un incidente de seguridad.

2. **Aplicación:**
   Este documento tiene como audiencia a todo el personal de la empresa que directa o indirectamente este involucrado en las actividades de monitoreo de los accesos y uso de los sistemas y/o redes de la empresa.

3. **Directrices:**
   Los principales procedimientos y actividades que deben realizarse son:
   a) Es importante que la utilización de cada recurso sea monitoreado para asegurar el uso óptimo del hardware y software.[8]

b) El monitoreo según lo establecido en [8] debe ser especifico dependiendo de los sistemas operativos, configuraciones particulares de hardware, aplicaciones, etc. Las variables a monitorear son las siguientes:
   - Utilización de CPU
   - Utilización de memoria
   - Tipo de transacción por porcentaje de utilización de CPU
   - Tasa de Entrada / Salida (físicas y de buffer) y utilización de dispositivo
   - Longitud de encolamiento (máximo y promedio)
   - Utilización de archivos de almacenamiento
   - Número de transacciones por segundo
   - Tiempo de respuesta a las transacciones
   - Número de logons y usuarios actuales
   - Número de nodos de red en uso

c) Se deben establecer umbrales y baselines de niveles de operación normal de las variables de monitoreo. [8]

d) Se debe monitorear que todos los umbrales esten por debajo del nivel al cual el recurso es sobre-utilizado, o debajo de lo acordado en los SLAs. [8]

e) Se debe monitorear el tiempo de respuesta de TI y servicios de red. La métrica de monitoreo se puede obtener mediante las siguientes maneras
   - Incorporando código específico dentro del software en aplicaciones cliente y servidores
   - Usando un agente distribuido de monitoreo de software
   - Usando un sistema de monitoreo pasivo, que rastree una muestra significativa del número de sistemas clientes. Este método confia en la conexión de sistemas de monitoreo específico en la red, frecuentemente se refieren como "sniffers", y son colocados en puntos apropiados en la red. Este puede monitorear y registrar todo el tráfico que pasa por un punto particular en la red, una vez que es registrado este tráfico, puede ser analizado para dar información detallada del tiempo de respuesta del servicio.

f) Deben ser establecidos procedimientos de monitoreo que faciliten el procesamiento de información. Tales procedimientos son necesarios para asegurar que los usuarios están realizando solo las actividades para las cuales están explícitamente autorizados. El nivel de monitoreo requerido para facilidades

individuales debe ser determinado mediante la evaluación de riesgos. Las áreas que deben ser consideradas son [13]:

1) Acceso autorizado, incluyendo lo siguiente:
   - Identificador de Usuario
   - Fecha y hora de evento
   - Tipo de evento
   - Archivo accedido
   - Programa o aplicación utilizada
2) Operaciones privilegiadas, tales como:
   - Uso de una cuenta de supervisor
   - Encendido y apagado de un sistema
3) Intentos de acceso no autorizados, tales como:
   - Intentos fracasados
   - Violación a las políticas de acceso
   - Alertas de sistemas de detección de intrusos
4) Sistemas de Alerta o fallas, tales como:
   - Consola de alertas o mensajes
   - Sistema de excepciones
   - Alarmas de administración de red

g) El resultado de las actividades de monitoreo debe ser revisado regularmente. La frecuencia de las revisiones depende del riesgo. Los factores de riesgo a ser considerados son [13]:
   - La criticidad de los procesos de aplicación
   - El valor, sensitividad o criticidad de la información en cuestión.
   - La experiencia sobre infiltraciones y uso incorrecto
   - Lo extenso de las interconexiones de sistemas

h) Se debe de registrar en bitácora , los eventos de seguridad relevantes, para apoyo en investigaciones futuras y monitorear el control de acceso. Los logs deben incluir los siguientes datos [13]:
1) Identificador de Usuario
2) Fecha y hora de conexión y desconexión
3) Posible localización e identificación de terminal
4) Registro de intentos exitosos y rechazados de acceso a sistemas
5) Registro de intentos exitosos y rechazados de acceso a información y otros recursos

i) Se debe llevar a cabo la revisión de bitácoras, lo cuál incluye el entendimiento de las diversas formas de amenaza y la manera en la cuál estas amenazas ocurren. Las bitácoras del sistema frecuentemente contienen un gran volumen de información, mucha de la cual no es relevante al monitoreo de seguridad. Para ayudar a identificar significativamente los eventos relacionados a la seguridad debe considerarse acciones como generar un segundo registro con los datos del primero previamente identificados, implementando utilerías del sistema o herramientas de auditorías del sistema.

Para efectuar estas actividades es necesario ubicar la responsabilidad sobre la revisión de las bitácoras; la separación de las funciones debe ser considerada entre las personas a hacer la revisión y aquellas cuyas actividades serán monitoreadas.

Se debe dar particular atención a la seguridad de bitácoras o registros en sí, debido a que pueden proveer de falsas conjeturas de seguridad. Los procedimientos que ayudan a proteger contra cambios no autorizados y problemas operacionales son [13]:

- Equipos y facilidades de almacenamiento de eventos (bitácoras) a ser desactivadas.
- Alteraciones de los tipos de mensajes que son almacenados
- Bitácoras de archivos a ser editados o borrados
- Medios de almacenamiento de bitácoras de archivo a ser consumido, fallidas o sobre-escritas

4. **Referencias:**

[**8**]. Office Governmet Commerce. *Best Practice for Delivery Support. ITIL. The key to Managing IT Service*. First edition, 2000.

[**13**]. British Standard Institute. *British Standard ISO17799-1*. 2da edition, 2003.

Capítulo 5

Conclusiones

En cuanto al marco de trabajo ITIL y el estándar ISO/IEC-17799

Para las compañías hoy en día la información es un activo, que como todo activo importante del negocio, tiene valor para la empresa y consecuentemente necesita ser debidamente protegida en cualquiera de sus formas de almacenamiento, escrita en papel, impresa, en un correo electrónico, en una base de datos, etc. El valor de la información es tan alto que debe ser protegida a través de la administración de la seguridad de la información contra una amplia gama de amenazas y vulnerabilidades que permita asegurar la continuidad del negocio, reducir al mínimo el posible daño al negocio y maximizar el retorno de inversión y oportunidades de negocio. Las amenazas pueden provenir de diferentes fuentes, como son humanas, con personas maliciosas externas o internas y no maliciosas (empleados ignorantes), desastres naturales (terremotos, inundaciones, incendios), fallas de equipos, errores de software, etc. Según [Manu00] en su libro "Seguridad, una introducción" plantea que el concepto de seguridad es multidimensional, significando cosas diferentes a diferentes personas en diferentes contextos. Debido a su complejidad, tanto la explicación como la atribución de responsabilidades y la medición de las actividades son frecuentemente poco fiables, o a lo menos discutibles. Esto tiene la peligrosa consecuencia de que la función de seguridad puede ser frecuentemente etiquetada como inadecuada o negligente. Muy a menudo, aquellos con una responsabilidad en seguridad no pueden defender sus decisiones y acciones contra "listasreclamaciones que están basadas en la ambigüedad de los actuales conceptos y definiciones de seguridad. ¿Cómo puede alguien afirmar, en ausencia de límites definidos, si "¿alguien o algo está seguro o no?". Por ello que proteger la información no solo es responsabilidad de quienes tienen la función de administrar un sistema, el correo electrónico, el firewall o de realizar los respaldos

de información de una base de datos, sino de todos aquellos que tienen algún tipo de contacto con la información de una compañía. Por ejemplo, es responsabilidad de cada usuario proteger la clave de acceso a los sistemas, o no divulgar información confidencial de una compañía, ya sea hablado o escrito en un correo electrónico, ante ésta problemática se adopta el estándar ISO/IEC-17799 el cual ayuda a determinar los controles necesarios para lograr un alto grado de seguridad en el activo de información de interés y otorgar credibilidad a los procesos, tecnologías y controles que son necesarios para el soporte de ambientes de seguridad de la información, pero aunque el estándar ISO/IEC-17799 posee fuertes en controles de seguridad, pero no establece como se debe realizar el flujo de procesos para la implementación de dichos controles, es aquí donde es necesario un marco de trabajo que ayude a implementar los procesos de TI y controles de seguridad para la información, por lo cual se determino que el mejor marco de trabajo para la gestión de servicios de TI es ITIL, ya que proporciona un conjunto de mejores prácticas extraídas de organismos punteros del sector público y privado a nivel internacional, las cuales han sido reunidas por la Oficina Gubernativa de Comercio Británica.

ITIL es fuerte en procesos de TI, pero limitado en seguridad y desarrollo de sistemas, y por su parte el estándar ISO/IEC-17799 es fuerte en controles de seguridad pero limitado en procesos de TI, por lo cual una interacción de ambos marcos es una combinación adecuada para lograr una alto grado de seguridad en la información, garantizando el desempeño óptimo y apropiado de la tecnología de información.

En cuanto a la necesidad y creación de políticas y normas de seguridad de información

La seguridad de la información es un proceso de gestión y no un proceso tecnológico, por ello es responsabilidad de los gerentes del negocio generar políticas de acuerdo a las necesidades de la empresa las cuales deben ser ejecutadas, controladas y auditadas como cualquier otro proceso de gestión de la compañía.

Para desarrollar e implementar un ambiente de seguridad adecuado, se debe establecer una política de seguridad, de la cual emane todas las directrices o normas que deben ser implantadas en la organización, a la cual todos los entes involucrados (procedimientos, máquinas, personas), deben adherir a ésta. Dicha política, se

sustenta en normas, las que establecen las definiciones para que sean desarrollados los procedimientos y metodologías que han de construirse para hacer funcionar, sea manual o automatizado, los mecanismos que permitirán mantener la plataforma bajo la protección y control que se haya definido en la política.

El funcionamiento de la seguridad de la red para proteger la información es un aspecto importante para las actuales empresas. Aunque el proceso de implementación de políticas completas para la seguridad de información puede resultar intimidante, ya que es frecuente que las personas involucradas con la seguridad de la información tengan una visión estrecha de lo que significa desarrollar políticas y normas de seguridad, pues no basta con escribirlas y pretender ponerlas en práctica, en ocasiones se incluye la asignación de responsables, realización de actividades de concientización para dar a conocerlas y, quizá, se supervise su cumplimiento.

Algunos problemas a los cuales se enfrenta la persona para la creación de las políticas y normas de seguridad de información es la falta de conocimiento y cultura en materia de seguridad de información, que existe por parte de algunas empresas, las cuales conciben a la seguridad de información como la implementación de equipo de tecnología tal como lo puede ser un firewall, lo cual es una idea errónea de seguridad de información ya que la tecnología sin un marco de gestión de servicios de TI y sin una metodología de implementación de controles de seguridad, resultará solamente en un gasto inadecuado, lo cual se traduce en pérdidas económicas para la empresa.

Cabe mencionar que una política eficaz de seguridad de la información corporativa es esencial para el buen funcionamiento de las empresas. El cumplimiento de estas políticas es muy importante hoy más que nunca puesto que las amenazas a la seguridad continúan multiplicándose en número y complejidad.

En cuanto al modelo de administración de seguridad de TI

El modelo propuesto de administración de seguridad de TI, tiene como objetivo cubrir los factores más importantes de seguridad los cuales son; integridad, confiabilidad y disponibilidad, a diferencia de modelos existentes, el modelo propuesto en este trabajo de tesis integra las mejores prácticas de tecnología de información dictadas por ITIL (en cuanto a materia de seguridad), el cual es el marco de trabajo con mayor

aceptación y calidad en gestión de servicios de TI, y los controles de seguridad de información determinados por el estándar ISO/IEC-17799, el cual es el estándar más completo en seguridad de información en la actualidad, de esta manera se obtienen normas que garantizan un alto grado de seguridad para los procedimientos básicos de seguridad de información tratados en esta tesis.

Por otra parte y de acuerdo con la obra "IT Governance: How Top Performers Manage IT Decision Rights for Superior Results" (Harvard Business School Press, Spring 2004),es importante mencionar que las empresas que disponen de un sistema de administración de la TI superior obtienen un beneficio del 25programa de administración insuficiente para los mismos objetivos estratégicos.

Por último cabe mencionar que la seguridad de información no es un método, es una cultura, la cual debe ir de la mano con el desarrollo de la organización, convirtiéndose de esta forma en una actividad en ejecución día con día, transformándose en políticas, normas, estándares y procedimientos, que combinados permitirán garantizar la confidencialidad, integridad y disponibilidad de la información.

5.1. Trabajo Futuro

Esta investigación y propuesta de modelo de administración de seguridad de TI, tuvo el propósito de generar un marco de referencia que pueda ser utilizado cualquier empresa preocupada en la seguridad de su información, las normas presentadas en este trabajo están dirigidas a una empresa de servicios de Telecomunicaciones, tal como lo es Alestra, sin embargo para otras empresas esta tesis representará un marco de referencia para la aplicación adecuada de normas de seguridad a sus procesos de TI mencionados a lo largo de este trabajo.

De acuerdo al modelo del proceso de Administración de Seguridad de Tecnología de Información propuesto en este proyecto de tesis (ver Figura 3.1), el proceso de la administración de la seguridad de la información es realizado en fases; las cuales, en la Figura 3.1 son ilustradas por medio de bloques. En este proyecto de tesis se enfocaron esfuerzos a la realización de las siguientes fases

1. **Fase de Análisis de Riesgo**: La cual es la fase fundamental para conocer a qué tipo de riesgos se encuentran expuestos los activos de información importantes para la empresa, y cuales son los procedimientos de seguridad

de información que afectaran directamente a la *Confidencialidad, Integridad y Disponibilidad* de la información. Es importante señalar que el Análisis de Riesgos fue realizado por el Área de Seguridad de Información de la empresa Alestra, dicho Análisis contiene información confidencial para la empresa por lo cual no puede ser incluida en este trabajo de tesis.

2. **Fase de Plan**: Es el primer paso en la investigación y creación de normas, lo que conlleva a la identificación de la necesidad de la norma, determinación del alcance y aplicabilidad de la norma, responsabilidad de la aplicación de la misma y garantizar la factibilidad de su implementación, y los controles de seguridad que minimizaran los efectos de algún posible incidente de tal manera que se garantice un nivel alto de seguridad de información.

3. **Evaluación**: Una de las tareas de la fase de evaluación es la de revisar la normas creadas para los diferentes procedimientos de seguridad de información, la cual ha sido cubierta en esta tesis.

Como trabajo futuro se puede observar que de acuerdo al Modelo de la Figura 3.1, se le puede dar continuidad a este trabajo, en las siguientes fases.

1. En la fase de Implementación, con las siguientes actividades:
   - Implementación práctica de las normas de seguridad para los distintos procedimientos de seguridad de información de interés para la empresa Alestra.
   - Concientización de los usuarios y operadores a quienes van dirigidas las normas de seguridad.
   - Manejo de incidentes, que pudieran presentarse en la implementación de las normas
2. En la fase de Evaluación:
   - Verificar el cumplimiento de las normas por parte de los involucrados
   - Verificar el cumplimiento de los SLAs
3. En la fase de Mantenimiento:
   - Verificar el tiempo de vigencia de la norma y realizar su revisión
   - Garantizar la integridad de la norma
   - Garantizar la documentación necesaria para mantener disponible la norma

Por otra parte, un trabajo futuro que se puede derivar de este y el cual es muy interesante es la implementación de ITIL bajo la perspectiva de marco de gestión de servicios, no solamente bajo la perspectiva de mejores prácticas de seguridad de información, que fue la perspectiva de interés del presente trabajo.

Glosario

A

activos Cualquier cosa que tenga valor para la organización, con las operaciones de negocio y sus continuidad, p. 1.

B

BSI British Standard Institute, p. 3.

C

Código Malicioso Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Un caballo de Troya es ejemplo de un código malicioso.

CI Componente de una infraestructura, p. 11.

Confidencialidad Asegurar que la información sea accesible solamente a quienes tienen acceso autorizado, p. 10.

D

Disponibilidad Asegurar que usuarios autorizados tengan acceso a la información y a activos asociados cuando lo requieran, p. 10.

droppers Es un programa que, cuando corre intentará instalar virus en el disco duro de la computadora., p. 55.

G

gusanos Similar al virus, con la característica adicional que busca subsistir en el Internet por cualquier medio a través de diversos mecanismos, ya sea por medio de correo electrónico o algún otro protocolo o aplicación a través de la red., p. 55.

I

Incidente Algún evento el cual no es parte de la operación estándar de un sistema y que tendrá impacto sobre el mismo, p. 13.

Integridad Salvaguardar la exactitud de la información y los métodos de procesamiento, p. 10.

ITIL Librería de Infraestructura de Tecnología de la Información, p. 2.

O

OLA (Operational Level Agreement) Acuerdos internos de la organización para cubrir entrega de servicios.

S

SLA (Service Level Agreement) Acuerdo formal entre entre el cliente y el proveedor de servicios, donde se especifica el nivel de servicio y los términos bajo los cuales es proporcionado un servicio al cliente.

T

Tecnología de Información Herramientas y métodos empleados para recabar, retener, manipular o distribuir información. Se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.

TI Tecnología de Información, p. 2.

troyanos Código malicioso que realiza acciones no esperadas o no autorizadas, normalmente maliciosas., p. 55.

V

virus Es un programa de computadora usualmente escondido dentro de otro aparentemente inocuo que produce copias de sí mismo y las inserta dentro de otros programas o archivos, y que usualmente ejecuta una acción maliciosa, tal como destruír datos., p. 55.

Bibliografía

[1] Christoper Alberts. *Managing Information Security Risk. The Octave Approach*. Fourth edition, 2003.

[2] Ross Anderson. *Security Engineering. A Guide to building Dependable Distributed System*. Fourth edition, 2002.

[3] Seymour Bosworth and M.E. Kabay. *Computer Security Handbook*. Fourth edition, 2002.

[4] Stuart Broderick. Introducción a las políticas, estándares y procedimientos de seguridad de la información. www.symantec.com, Mayo 2003.

[5] Office Government Commerce. *Best Practice for Security Management. ITIL. The key to Managing IT Service*. 1era edition, 2000.

[6] Office Government Commerce. *Best Practice for Service Support. ITIL. The key to Managing IT Service*. 1era edition, 2000.

[7] Office Government Commerce. Capacity planing. In Office Government Commerce, editor, *Best Practice for Service Support. ITIL. The key to Managing IT Service*. First edition, 2000.

[8] Office Governmet Commerce. *Best Practice for Delivery Support. ITIL. The key to Managing IT Service*. First edition, 2000.

[9] Roberto Hernández. *Metodología de la Investigación*. Third edition, 2003.

[10] Debra S. Herrman. *A Practical Guide to Security Engineering and Information Assurance*. Second edition, 2002.

[11] Patrick D. Howard. The security policy life cycle: Funtions and responsabilities. In Tipton & Krause, editor, *Information Security Management Handbook*. CRC Press LLC, 2003.

[12] British Standard Institute. *British Standard BS 7799-2*. 2da edition, 2003.

[13] British Standard Institute. *British Standard ISO 17799-1*. 2da edition, 2003.

[14] Office of Government Commerce. *Best Practice for ICT Infrastructure Management. ITIL The key to Managing IT services.* Office of Government Commerce, first edition, 2002.

[15] Symantec. Aumento en las amenazas combinadas, vulnerabilidades y ataques en internet. www.symantec.com, Octubre 2003.