UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA DE DERECHO

MONOGRAFÍA

"FUNDAMENTOS LEGALES PARA ELABORAR UN SISTEMA DE SEGURIDAD INFORMÁTICA EN LA BASE DE DATOS DEL GOBIERNO AUTÓNOMO MUNICIPAL DE LA PAZ"

"PARA OPTAR AL TÍTULO ACADÉMICO DE LICENCIATURA EN DERECHO"

POSTULANTE	**:**	Florencio Morales Mamani.
TUTOR ACADEMICO	**:**	Dr. Hernán Clavel Salazar.
INSTITUCION	**:**	Gobierno Autónomo Municipal de La Paz**.**

LA PAZ - BOLIVIA

2013

DEDICATORIA

A la Facultad de Derecho por hacer posible mi formación bajo los sagrados principios que rige la Universidad Mayor de san Andrés.

A mis padres y hermano, principalmente A mi madre por sus palabras que me fortalecieron para seguir adelante y así lograr mi superación.

F.M.M.

AGRADECIMIENTO

Mi profundo agradecimiento a las autoridades facultativas y a los docentes de la carrera de Derecho de ellos aprendí, sobre todo a los docentes por el esforzado trabajo de formar nuevas generaciones de profesionales que indudablemente, contribuirán en el desarrollo de nuestro país.

Mi particular agradecimiento al Dr. Hernán Clavel Salazar, quien gentilmente acepto ser mi tutor académico en el presente trabajo, por su conocimiento, su compromiso y su cooperación.

Mis agradecimientos al Gobierno Autónomo Municipal de La Paz por haberme brindado la oportunidad de trabajar en esa prestigiosa institución.

F.M.M.

PROLOGO

Quiero comenzar este honor al que al que se me ha invitado, señalando que el presente trabajo de investigación es un documento que aporta el postulante, donde se sintetiza la experiencia del postulante, se plasma en una descripción, análisis formal y útil acerca de un problema concreto de la realidad, solventando con sus conocimientos académicos y por otro lado es una visión crítico- constructiva de su formación académica, en contraste con las experiencias del ejercicio profesional desarrollado. Es decir este trabajo de investigación ayudara, que surja la seguridad Informática en el campo del Derecho Informático que sea ha permitido desarrollar un documento profesional y metodológico que refleja las características profesionales y contiene asimismo una propuesta del postulante.

Para finalizar puedo mencionar que varios e importantes trabajos se han presentado sobre las actividades que se desarrollan en el Gobierno Autónomo Municipal de La Paz y por ende es el reflejo de la capacidad intelectual del postulante que realizo el presente trabajo de investigación.

La Paz, marzo de 2013.

Dr. Vladimir Gutiérrez Ramírez
Dirección jurídica – G.A.M.L.P.

INDICE GENERAL

Diseño de la investigación	**Pág.**
1.- Motivación	1
2.- Identificación del problema	1
3.- Fundamentación o justificación	2
4.- Objetivos	3
4.1.- Objetivo General	3
4.2.- Objetivo Especifico	4
5.- Método de la Investigación	4
5.1.- Métodos Generales	4
5.1.1.- Método Deductivo	4
5.1.2.- Método Comparativo	4
5.1.3.- Método Analítico Sintético	5
5.2.- Métodos Específicos	5
5.2.1.- Método de las Construcciones Jurídicas	5
5.2.2.- Técnicas a Utilizar	5
5.2.3.- Entrevista	5
6.- Delimitación del tema	6
6.1.- Delimitación Temática	6
6.2.- Delimitación Espacial	6
6.3.- Delimitación Temporal	6
7.- Revisión Bibliográfica	6

CAPITULO I

I.1.- Antecedentes históricos	7
I.2.- Marco teórico o de referencia	9
I.2.1.- Marco teórico	9
I.2.2.- Marco histórico	11
I.2.3.- Marco conceptual	12
I.2.3.3.- Informática	13

I.2.4.- Marco jurídico 13
I.2.4.1.- Legislación Nacional 13
I.2.4.2.- Legislación Comparada 17
I.3.- Planteamiento del problema 20

CAPITULO II

FUNDAMENTOS TEÓRICOS, CONCEPTUALES Y TÉCNICAS DE LA SEGURIDAD INFORMÁTICA Y SU IMPLEMENTACIÓN.

II.1.- Seguridad Informática 21
II.1.1.- Análisis del objeto de la seguridad informática 22
II.1.2.-Sistema de seguridad 25
II.1.3.-De quien debemos protegernos 26
II.1.4.-Que debemos proteger 27
II.1.5.-Relacion operatividad Seguridad 29
II.2.- Seguridad Física 31
II.2.1.-Tipos de desastres 32
II2.2.-Incendios 33
II.2.3.-Seguridad del equipamiento 34
II.2.4.-Inundaciones 35
II.2.5.-Condiciones climatológicas 35
II.2.6.-Terremotos 36
II.2.7.-Robo 36
II.2.8.- Fraude 36
II.2.9.-Sabotaje 37
II.2.10.-Control de accesos 37
II.2.11.-Control de personas 37
II.2.12.-Control de vehículo 39
II.2.13.-Utilizacion de detectores de metal 39
II.2.14.-Utilizacion de sistemas Biométricos 39
II.2.15.-Huella digital 40
II.2.16.-Verificacion automática de firmas 40
II.2.17.-Proteccion electrónica 41
II.2.18.-Detector ultrasonido 41

II.2.19.-Circuito cerrado de televisión 41
II.2.20.-Edificios Inteligentes 42
II.3.- Seguridad lógica 42
II.3.1.-Control de acceso 43
II.3.2.-Roles 44
II.3.3.-Transacciones 44
II.3.4.-Limitaciones a los servicios 44
II.3.5.-Modalidad de acceso 44
II.3.6.-Ubicación y horario 45
II.3.7.-Encriptacion 45
II.3.8.-Listas de control de acceso 46
II.3.9.-Limites sobre la interface de usuario 46
II.3.10.-Etiquetas de seguridad 46
II.3.11.-Dispositivos de control de puertos 46
II.3.12.-Firewalls o puertos de seguridad 47
II.3.13.-Niveles de seguridad informática 47
II.3.13.1.-Nivel A: Protección verificada 47
II.3.13.2.-Nivel B1: Seguridad etiquetada 48
II.3.13.3.-Nivel B2: Protección estructurada 48
II.3.13.4.-Nivel B3: Dominios de seguridad 48
II.3.13.5.-Nivel C1: Protección discrecional 49
II.3.13.6.-Nivel C2: Protección de acceso contralado 50
II.3.13.7.-Firewalls. 50
II.3.13.8.-Beneficio de un Firewalls 51

CAPITULO III

POLITICAS DE SEGURIDAD.

III.1.1.-Politicas de seguridad informática 54
III.1.2.-Evaluacion de riesgos 56
III.1.3.-Identificacion de amenaza 59
III.1.4.-Evaluacion de costos 60
III.1.5.-Valor intrínseco 62

III.1.6.-Costos derivados de la pérdida 63
III1.7.-Puntos de equilibrio 63
III.2.- Estrategias de Seguridad 64
III.2.1.-Implementacion 66
III.2.2.-Auditoria y control 69
III.2.3.-Auditoria 71
III.2.3.1Auditoria interna y Auditoria externa 72
III.2.4.-Alcance de la auditoria informática 74
III.2.5.-Caracteristicas de la auditoria Informática 74
III.2.6.-Sintomas de necesidad de una auditoria 75
III.2.7.-Objetivos fundamentales de la auditoria informática; operatividad 77
III.2.8.-Revicion de controles de la gestión informática 78
III.2.9.-Auditoria informática de explotación 79
III.2.10.-Auditoria informática de desarrollo de proyectos o aplicaciones 81
III.2.11.-Auditoria informática de sistemas 83
III.2.12.-Auditoria informática de comunicaciones y redes 84
III.2.13.-Auditoria de la seguridad informática 85

CAPITULO IV

IV.1.- Propuestas del Trabajo Dirigido 88
IV.2.- Dimensión y alcance de la propuesta 89
IV.3.- Conclusiones 90
IV.4.- Recomendaciones 90
IV.5.- Bibliografía 91

INTRODUCCION

La temática de la seguridad informática en relación a la base de datos de la entidad pública ejemplo el Gobierno Autónomo Municipal de La Paz, tomadas como muestra para la investigación, se verifica que la entidad pública, es evidente la inexistencia de normativa específica en el tema de investigación, y mi persona sugiere la importancia de desarrollar y proponer alguna normativa que permita regular la seguridad informática en las entidades públicas, lo cual con el aporte de los mismos se desarrolla en esta investigación.

Se conoce que existen propuestas de ley referidas al tema informático en el parlamento, por cuestiones meramente políticas, desinterés en el tema, continúan en suspenso.

La vital importancia deriva de la inexistencia de una normativa específica que regule la seguridad informática de nuestros datos que se encuentran depositados en la base de datos de la entidad pública, tal falencia genera un alto nivel de riesgo de que la información, por diversos factores sean perdidos, modificados, sustraídos, razón por la cual es necesario la protección legal, en la presente investigación se desarrolla, propone una normativa para regular le seguridad informática que es de vital importancia proteger los derechos de la sociedad en general de nuestro país.

El presente trabajo de investigación fue realizada por mi persona Florencio Morales Mamani y también me colaboro con sus conocimientos, ideas el Dr. Vladimir Gutiérrez Ramírez de la dirección jurídica del Gobierno Autónomo Municipal de La Paz.

ELECCIÓN DEL TEMA DE LA MONOGRAFÍA.

"FUNDAMENTOS LEGALES PARA ELABORAR UN SISTEMA DE SEGURIDAD INFORMÁTICA EN LA BASE DE DATOS DEL GOBIERNO AUTÓNOMO MUNICIPAL DE LA PAZ"

1.- MOTIVACIÓN.

La presente investigación es una oportunidad en el que el estudiante egresado de la facultad de Derecho se constituye en un observador de la realidad nacional, por ello esta experiencia sirve de motivación para profundizar cualquier tema de investigación en la vida profesional.

Como una fuente de investigación especifica para el postulante, el tema de investigación es importante, por la inseguridad informática en las entidades públicas y además permite sugerir algunas alternativas de solución al problema de la seguridad informática.

Finalmente se debe considerar que el tema abordado en la presente monografía es de interés nacional, importante para la seguridad informática de nuestro país.

2.- IDENTIFICACIÓN DEL PROBLEMA.

Nuestra legislación en la materia de derecho informático referida al tema de seguridad informática se encuentra relegada, de esta manera se identifica la inexistencia de una normativa general y uniforme que regule la seguridad de los datos que se encuentran depositados en la base de datos de la entidad pública, ejemplo el Gobierno Autónomo Municipal de La Paz generando un alto nivel de riesgo que la información, por diversos factores sean perdidas, modificadas, sustraídas, siendo dicha información de gran importancia para los ciudadanos, empresas y Estado.

De esa manera se hace necesaria la protección de nuestros datos; la protección legal utilizando normativas legales, los cuales permitan elaborar un sistema de seguridad informática en la base de datos de la entidad publicas de nuestro país.

3.- FUNDAMENTACIÓN O JUSTIFICACIÓN DEL TEMA.

La motivación esencial para el desarrollo de este tema, es conocer si nuestra información depositada en la base de datos de la entidad pública, ejemplo el Gobierno Autónomo Municipal de La Paz, está jurídicamente protegida con una normativa que regule la seguridad informática, en caso de que nuestra legislación cuente con alguna normativa conocer si se aplica, para así plantear la elaboración y uniformidad de normativas legales de seguridad informática los cuales permitan una mejor protección de la base de datos de la entidad pública; de esa manera se evidencia falta de conocimiento, vacíos jurídicos, en la protección de nuestra información que es manejada por la entidad pública, como por ejemplo el Gobierno Autónomo Municipal de La Paz.

Se justifica porque existe deficiencia respecto a la seguridad de nuestra información, incertidumbre jurídica respecto a la seguridad e integridad.

Es por eso se plantea y propone en esta investigación el desarrollo de una normativa que regule la seguridad informática mediante la aplicación de normativas legales los cuales garanticen la seguridad de nuestra información.

La principal cualidad de este trabajo de investigación es la exploración respecto al tema de la seguridad informática, para así coadyuvar y proponer la uniformidad, regulación de la seguridad informática, que es necesaria para el resguardo de nuestros datos, será herramienta de gran beneficio para los responsables del manejo de la base de datos de la entidad pública, como el Gobierno Autónomo Municipal de La Paz que no es muy seguro, el manejo de la información de los ciudadanos que manejan los funcionarios de la alcaldía.

Una de las principales falencias es la obtención de la información en la entidad públicas ya que se niega al acceso de la misma, falta de conocimiento, respecto al tema por parte de nuestras autoridades, lo cual lo único que provoca es el retraso frente a estas necesidades.

El presente trabajo se fundamenta en la necesidad de realizar un análisis sobre el enunciado del problema, nuestra legislación en la materia de derecho informático referida al tema de seguridad informática se encuentra relegada, de esta manera se identifica la inexistencia de una normativa, en caso de que nuestra legislación cuente con alguna normativa conocer si se aplica la normativa general y uniforme que regule la seguridad de los datos que se encuentran depositado en la base de datos de la entidad pública del Gobierno Autónomo Municipal de La Paz, generando un alto nivel de riesgo que la información, por diversos factores sean perdidas, modificadas, sustraídas, siendo dicha información de gran importancia para los ciudadanos, empresas y Estado.
De esa manera se hace necesaria la protección de nuestros datos; la protección legal utilizando fundamentos legales los cuales permitan elaborar un sistema de seguridad informática en los datos del Gobierno Autónomo Municipal de La paz.

4.- OBJETIVOS.

4.1. OBJETIVO GENERAL.

Demostrar el problema de la inseguridad informática en la que se encuentran nuestra información depositada en la base de datos del Gobierno Autónomo Municipal de La Paz para analizar, identificar la ineficacia e inexistencia de una normativa específica que regule la seguridad informática, para prevenir las consecuencias que puede acarrear o consecuencias que pueden perjudicar a la sociedad.

4.2. OBJETIVOS ESPECIFICOS.

Demostrar el problema de la inseguridad informática en la que se encuentra nuestra información depositada en la base de datos del Gobierno Autónomo Municipal de La Paz.

- Analizar la inseguridad informática tomando como parámetro la normativa vigente respecto al tema.

- Identificar la ineficacia, inexistencia de una normativa especifica que regule la seguridad informática.

- Proponer normas legales, dentro el área informática, así como también instrumentos legales para la protección de la información.

- Elaborar un sistema, de seguridad informática mediante políticas, planes de seguridad que nos garantice la seguridad jurídica de la información.

5.- **MÉTODO DE LA INVESTIGACIÓN.**

5.1 .- <u>MÉTODOS GENERALES</u>.

5.1.1.- MÉTODO DEDUCTIVO.- Nos permitirá partir la investigación de principios y teorías generales para conocer el fenómeno de la falencia de una normativa y la inseguridad informática en la que se encuentra la información depositada en la base de datos del Gobierno Autónomo Municipal de La Paz.

5.1.2.- MÉTODO COMPARATIVO.- Nos permitirá conocer las diferencias, similitudes, el retraso en el que se encuentra nuestra legislación en materia de seguridad informática.

5.1.3.- MÉTODO ANALÍTICO SINTÉTICO.- Nos permitirá analizar la inseguridad informática en la que se encuentra la información depositada en la base de datos del Gobierno Autónomo Municipal de La Paz, descomponiendo la misma en sus partes constitutivas que se expresan en factores, legales, técnicos; concernientes al derecho informático, penal, administrativo, civil, etc. Para luego realizar una integración sintética de los factores constitutivos para así determinar el objeto de investigación.

5.2 .- METODOS ESPECIFICOS.

5.2.1.- METODO DE LAS CONSTRUCCIONES JURIDICAS.

Este método nos permitirá construir soluciones a la vez generales y precisas para la diversidad de los casos individuales que exigen regulación, independientemente de las características particulares de cada uno. Consiste en explicaciones lógicas de las soluciones legales y conforman el nivel más sofisticado de la norma jurídica.

5.2.2.- TÉCNICAS A UTILIZAR.

- **LA ENTREVISTA**, es un encuentro social en que se tiene una conversación.
  Hay que asegurar, entonces, una situación grata, de modo que la entrevista se desarrolle fácilmente.
  La entrevista estructurada o dirigida se realiza con un cuestionario y con una cedula que se debe llenar a medida que se desarrolla. Las respuestas se transcriben tan y como las proporciona el entrevistado, por lo tanto las preguntas siempre se plantean con el mismo orden.

De esa manera utilizaremos la técnica cualitativa, mediante la entrevista estructurada a los encargados del manejo de la base de datos y responsables en el área informática, mediante esta técnica obtendremos Riqueza informativa, intensiva, contextualizada y personalizada también se tendrá acceso a información difícil de observar respecto al tema, nos facilitara, aclarar, responder los cuestionamientos.

6.- DELIMITACION DEL TEMA DE LA MONOGRAFÍA.

La delimitación me permitirá establecer los límites, el alcance y los recursos establecidos en los siguientes parámetros:

- **6.1. DELIMITACIÓN TEMATICA.**

  La investigación será enfocada de manera general desde el punto de vista jurídico del derecho público de manera específica, al derecho informático en el área de la seguridad informática.

- **6.2. DELIMITACIÓN ESPACIAL.**

  Se tomara como campo de investigación a las siguientes entidades públicas como ser el Gobierno Autónomo Municipal de La Paz y Servicio de Impuestos Nacionales de la ciudad de La Paz.

- **6.3. DELIMITACIÓN TEMPORAL.**

  El parámetro de estudio se considera información comprendida entre el periodo de la gestión 2009 al 2012.

7.- REVISIÓN BIBLIOGRÁFICA.

Mediante la utilización de esta técnica, pude recabar información a nivel de biblioteca, apuntes, hemerotecas, diccionarios, páginas de internet, periódicos y otros con la finalidad de seleccionar material bibliográfico destinado a enriquecer el presente trabajo de investigación de este proyecto.

CAPITULO I

I.1.- ANTECEDENTES HISTÓRICOS DEL PROBLEMA.

Las sociedades humanas se caracterizan por el constante cambio, el que cada día nos sorprende más por su rapidez y profunda incidencia en el desarrollo de patrones de conducta social, creando entre las personas nuevos modos de interacción. Sin embargo, no estamos en presencia únicamente de progreso científico o tecnológico, sino que el cambio involucra las creencias, las actitudes psicológicas, el ámbito económico y político; en suma, la forma de convivir en el mundo.

Es decir, estamos viviendo un verdadero cambio social que modifica irreversiblemente los modos de conducta en sociedad.

Sin lugar a duda, estos cambios sociales profundos se tienen que reflejar a través de modificaciones serias en el ordenamiento jurídico, como sucede por ejemplo, con el surgimiento de la legislación medioambiental o las normas que rigen a las tecnologías de la información. Ante ello, el Derecho no puede negarse a progresar, entendiendo que éste progreso cuando es capaz de interpretar mejor las necesidades humanas y de adaptarse en forma más perfecta a lo que de él se requiere para el bien común, la paz, la justicia y el progreso.

Por tal motivo, en un cambio que consiste en la modernización del sistema social, sin sustituir los valores y las estructuras fundamentales existentes en la comunidad, el Derecho debe permitir o facilitar el uso oportuno de recursos humanos, naturales, financieros, científicos y otros, existentes en la comunidad.

La revolución tecnológica ha redimensionado las relaciones entre los hombres. Estamos en una sociedad donde las tecnologías de la información han llegado a ser la figura representativa de nuestra cultura, hasta el punto de que para designar el marco de nuestra convivencia se alude reiteradamente a la expresión "sociedad de la información".

Frente a las cada vez mayores repercusiones de la informática en el Derecho muchos de los problemas que se suscitan no se satisfacen con las soluciones jurídicas tradicionales, muchas de ellas insuficientes y obsoletas hoy en día, debido a que los conceptos y categorías básicos de la ciencia jurídica que surgieron en la edad moderna y en la codificación actual, han variado.

Ello obliga a tener una actitud reflexiva crítica y responsable ante los nuevos problemas que acarrea la tecnología de la información, aunque se haga necesario que los estudiosos del Derecho adopten una conciencia tecnológica y se familiaricen con aspectos científicos e informáticos. De esta forma se presenta el acercamiento de dos disciplinas inmutables e irreconciliables entre sí como lo son el Derecho y la Informática, las cuales, si bien diferentes en su naturaleza, no lo son tanto en sus propósitos de prestar servicio al hombre y propender a una sociedad más justa y eficiente.

Por esta razón, se deben diseñar nuevos instrumentos de análisis y marcos conceptuales para adaptarse a las exigencias de una sociedad en transformación, hay que construir una ciencia del Derecho abierta y comprometida con las respuestas a las nuevas necesidades de quienes vivimos en la era de la informática.

Esta nueva ciencia solo por dar un ejemplo debe tomar muy en cuenta el valor probatorio de los documentos informáticos, pues desde hace mucho tiempo y más aun de aquí en adelante los documentos informáticos se convertirán en un grave problema, por la dudosa procedencia y la falta de garantías de los mismos.

Es por esta razón y más aun por el retraso de la seguridad informática, que vive Bolivia, que considero muy necesario presentar este trabajo para así poder orientar que pasos se pueden tomar en el difícil mundo de la informática, para poder dar a los datos, documentos informáticos un valor que garantice y tranquilice a cualquier persona para defender sus derechos.

I.2.- MARCO TEÓRICO O DE REFERENCIA.

I.2.1 MARCO TEÓRICO.

Mi investigación se guiara en la Teoría Positivista, que es el conjunto de conocimientos previos sobre un determinado problema; por lo que dicha corriente es la que fundamentara mi trabajo.

Tomando el concepto netamente se seguridad Fayol dice: "…salvaguardar propiedades y personas contra el robo, fuego, inundación contrarrestar huelgas y felonías, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Es generalmente hablando, todas las medidas para conferir la requerida paz y tranquilidad.

Las medidas de seguridad a las que se refiere Fayol, sólo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese: los equipos, ni siquiera el empleado. Con la aparición de los "cerebros electrónicos", esta mentalidad se mantuvo, porque ¿quién sería capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?

O.I.T. Seguridad social un nuevo consenso capítulo IV igualdad de genero, informe de la comisión de la seguridad social conferencia internacional del trabajo, 89 ava reunión 2001

Podemos entender como seguridad informática un estado de cualquier sistema (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- Integridad: La información sólo puede ser modificada por quien está autorizado.
- Confidencialidad: La información sólo debe ser legible para los autorizados.
- Disponibilidad: Debe estar disponible cuando se necesita.
- Irrefutabilidad: (No-Rechazo o No Repudio) Que no se pueda negar la autoría.

Hoy, la seguridad, desde el punto de vista legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera. Este proceso ha conseguido importantes logros en el contexto internacional, en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre Seguridad aunque en Bolivia esta relegado.

En cambio desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

I.2.2. MARCO HISTÓRICO.

Sin lugar a dudas, estos cambios sociales profundos se tienen que reflejar a través de modificaciones serias en el ordenamiento jurídico, como sucede por ejemplo, con el surgimiento de la legislación medioambiental o las normas que rigen a las tecnologías de la información. Ante ello, el Derecho no puede negarse a progresar, entendiendo que

éste progreso cuando es capaz de interpretar mejor las necesidades humanas y de adaptarse en forma más perfecta a lo que de él se requiere para el bien común, la paz, la justicia y el progreso.
Por tal motivo, en un cambio que consiste en la modernización del sistema social, sin sustituir los valores y las estructuras fundamentales existentes en la comunidad, el Derecho debe permitir o facilitar el uso oportuno de recursos humanos, naturales, financieros, científicos y otros, existentes en la comunidad.

Este cambio no es producto de un acaso, sino del afán consiente de las personas por buscar soluciones satisfactorias a sus problemas y necesidades. Es así como nadie podría desconocer que el desarrollo de la ciencia y la tecnología es una de sus importantes causas directas e inmediatas.

La revolución tecnológica ha redimensionado las relaciones entre los hombres. Estamos en una sociedad donde las tecnologías de la información han llegado a ser la figura representativa de nuestra cultura, hasta el punto de que para designar el marco de nuestra convivencia se alude reiteradamente a la expresión "sociedad de la información".

Frente a las mayores repercusiones de la informática en el Derecho, muchos de los problemas que se suscitan no se satisfacen con las soluciones jurídicas tradicionales, muchas de ellas insuficientes y obsoletas hoy en día, debido a que los conceptos y categorías básicos de la ciencia jurídica que surgieron en la edad moderna y en la codificación actual, han variado.

Ello obliga a tener una actitud reflexiva crítica y responsable ante los nuevos problemas que acarrea la tecnología de la información, aunque se haga necesario que los estudiosos del Derecho adopten una conciencia tecnológica y se familiaricen con aspectos científicos e informáticos. De esta forma se presenta el acercamiento de dos disciplinas inmutables e irreconciliables entre sí como lo son el Derecho y la Informática, las

cuales, si bien diferentes en su naturaleza, no lo son tanto en sus propósitos de prestar servicio al hombre y proponer a una sociedad más justa y eficiente.

Por esta razón, se deben diseñar nuevos instrumentos de análisis y marcos conceptuales para adaptarse a las exigencias de una sociedad en transformación, hay que construir una ciencia del Derecho abierta y comprometida con las respuestas a las nuevas necesidades de quienes vivimos en la era de la informática.

I.2.3 MARCO CONCEPTUAL

I.2.3.1.- La seguridad informática: es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema**.**

"El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales), Control y Autenticidad de la información manejada por computadora."

I.2.3.2.- BASE DE DATOS.

Se puede definir a este bien como cualquier conjunto de datos organizados para su almacenamiento en la memoria de un ordenador o computadora diseñado para facilitar su mantenimiento y acceso de una forma estándar, los datos suelen aparecer en forma de texto, números o gráficos.

Seguridad Informática: Según diccionario enciclopédico Océano Uno, Edición 1991.

Base de Datos: Según apuntes de lecciones de derecho informático de autor Dr. Cesar Burgoa Rodríguez.

Informática: Según diccionario jurídico del autor Manuel Osorio, editorial heliasta, edición 2007.

Información: Según apuntes de lecciones de derecho Informático del autor Dr. Cesar Burgoa Rodríguez.

I.2.3.3.- I NFORMÁTICA.-

Denominación de la técnica informativa basada en el rigor lógico y en la automatización posible, al punto de utilizar con frecuencia y dentro de las posibilidades, las computadoras se diversifican en diferentes especies como ser metodológica, que elabora los métodos de programación y exploración de computadoras.

La **Información** "es una agregación de datos que tiene un significado específico más allá de cada uno de éstos" y tendrá un sentido particular según como y quien la procese, Ejemplo: 1, 9, 8 y 7 son datos; su agregación 1987 es Información.

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

I.2.4 MARCO JURÍDICO.

I.2.4.1 LEGISLACIÓN NACIONAL.

- **NUEVA CONSTITUCIÓN POLÍTICA DEL ESTADO PLURINACIONAL.**

A). ARTÍCULO 130.- I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

A). 1.- Análisis del articulo 130 (Nueva Constitución Política del Estado Plurinacional**).**

En este articulo se menciona que cualquier persona que este impedido de conocer, objetar u obtener la eliminación de los datos que estén registrados en cualquier medio físico, señala que pueden interponer la acción de protección de privacidad, ósea menciona que nadie puede eliminar o modificar los datos que estén registrados en la base de datos de cualquier medio físico de una entidad pública.

B). ARTÍCULO 131.- **I**. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la Acción de Amparo Constitucional.

II. Si el tribunal o juez competente declara procedente la acción ordenara la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.

III. La decisión se elevara, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de veinticuatro horas siguientes a la emisión del fallo, sin que por ellos se suspenda la ejecución.

IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad la autoridad judicial que no proceda conforme con lo dispuesto por este articulo quedara sujeta a las sanciones previstas por la ley.

B). 1.- Análisis del articulo 131 (Nueva Constitución Política del Estado Plurinacional).

En este artículo señala que el tribunal o juez declara procedente la acción y ordenara la eliminación o rectificación de los datos cuyo registro fue impugnado. Ósea menciona que si una persona observa que sus datos registrados estén borrados o modificados puede solicitar al tribunal o juez sean corregidos.

Nueva Constitución Política del Estado Plurinacional.

- **LEY No. 1768 CÓDIGO PENAL BOLIVIANO.**

Asimismo, el Código Penal Boliviano, texto ordenado según ley No 1768 de 1997, incorpora en el Título XII, Capitulo XI destinado a los Delitos Informáticos, los siguientes Artículos.

1.- ARTÍCULO.- 363 bis. (Manipulación Informática). El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzcan a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una trasferencia patrimonial en perjuicio de terceros, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

1. 1.- Análisis del artículo 363 bis (Código Penal Boliviano).

En este articulo se menciona que si una persona tiene la intención de obtener un beneficio para el u otra persona y por lo cual manipule la transferencia de datos informáticos incorrectos o modifique los datos de una información, ocasionando un perjuicio al titular de la información o terceras personas, deben ser sancionados con la reclusión de uno a cinco años y multa de sesenta a doscientos días

2.- ARTÍCULO.- 363 ter. (Alteración, acceso y uso indebido de datos informáticos). El que sin estar autorizado se apoderare, acceda, Utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

2. 1.- Análisis del articulo 363 ter. (Código Penal Boliviano).

En este articulo menciona que cualquier persona que no este autorizado a modificar, suprimir o apoderarse de una información que este almacenado en una computadora o cualquier soporte informático debe ser sancionado con prestación de trabajo hasta un año o multa hasta doscientos días por ocasionar un perjuicio al titular de una información.

Hoy en día se puede verificar que en la prefectura de Cochabamba **Borraron información de las computadoras prefecturales** de Cochabamba así lo denuncio el secretario general de la prefectura de Cochabamba David Herrera, publicado en el periódico el Diario en fecha 04/09/08 (**ver Anexos**).

- **LEY No. 1322 DERECHOS DE AUTOR.**

1.- ARTÍCULO 6º.- Esta Ley protege los derechos de los autores sobre sus obras literarias, artísticas y científicas, cualesquiera que sean el modo o la forma de expresión empleado y cualquiera sea su destino, ella comprende especialmente:

l) Los programas de ordenador o computación (soporte lógico o software) bajo reglamentación específica.

Es objeto de la protección de esta Ley toda creación literaria, artística, científica, cualquiera sea la forma de expresión y el medio o soporte tangible o intangible actualmente conocido o que se conozca en el futuro.

1.1.- Análisis del artículo 6º (Derechos de autor).

En este artículo se menciona que se protege los derechos de los autores sobre sus obras artísticas, científicas y otros, ósea si un dato de información mediante los programas de ordenador o computación son modificados deben ser protegidos mediante esta ley.

Ley No. 1768 Código Penal Boliviano

Ley No. 1322 Derechos de Autor.

I.2.4.2 LEGISLACION COMPARADA.

- **1.3. ARGENTINA.-**

LEY NO. 25506 DE 14/11/2001
AUTORIDAD LICENCIANTE

Jefatura Gabinete Ministros en Administración Pública, la Firma digital es el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante encontrándose ésta bajo su absoluto control.

Firma electrónica: conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital.

Análisis de la legislación comparada (Argentina).

Mediante esta legislación de Argentina se menciona que la jefatura de ministros en el área de administración pública realiza la firma digital y por lo cual se aplica en documentos digitales que requiere información del firmante para que sea protegida la firma digital.

- **1.4. CHILE.-**

LEY No. 1979 vigencia de: 12/4/2002 de 26 Artículos.
Similares principios: libertad, equivalencia

Contiene definiciones de firma electrónica y firma electrónica avanzada. Ésta es la que emite un Prestador acreditado.

Entidad acreditadora: Subsecretaría de Economía, Fomento y Reconstrucción.
Igual valor para actos y contratos; excepciones:
-Que la ley exija solemnidad, derecho de familia, Necesaria concurrencia personal de la parte.
-Los instrumentos públicos requieren ser avanzada de la certificación de autoridades o Funcionarios de órganos del Estado se realiza por los respectivos ministros.
-Prestadores de servicios de certificación.
-Persona jurídica nacional o extranjera Pública o privada, responsabilidad del usuario: por daños y perjuicios salvo uso fraudulento o indebido del certificado.
Prestadores acreditados: obligados a contratar y mantener seguro por 5.000 unidades de fomento como mínimo, en ningún caso es responsable el Estado.
La entidad acreditadora ejerce inspecciones y Puede contratar personal técnico.Se establecen definiciones, procedimiento de acreditación y requisitos

Análisis de la legislación comparada de (Chile).

Mediante esta legislación se menciona que contiene definiciones de firma electrónica y es emitido por un prestador acreditado y el usuario es el responsable por los daños y perjuicios ocasionados a la ciudadanía.

- **1.5. ESPAÑA.-**

  LEY No. 15/1999

Desde el 13 de diciembre de 1999, existe en España un marco legal de obligado cumplimiento para las empresas y trabajadores autónomos españoles, cuya misión fundamental es velar por la protección de los datos de carácter personal. Éste texto es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), oficializada en el BOE núm. 298, del 14 de diciembre de 1999.

Históricamente, ésta norma sustituyó a la que se conocía como LORTAD (Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal). En líneas generales es un amplio marco legal donde se describen la necesidad de proteger la privacidad de las personas. Concretamente, en lo referente a la adquisición, tenencia, tratamiento y cesión de ficheros que contengan datos de carácter personal, tales como nombre, apellidos, número de cuenta bancaria, así como datos especialmente protegidos, como la ideología religiosa, datos relativos frecuentemente, las gerencias de las empresas enfocan la conformidad con la LOPD como un problema, como una traba, como una necesidad de gastar recursos financieros por imperativo legal. El motivo de éste artículo es propiciar una visión a gerentes y responsables, así como a usuarios en general, de que alinearse con este texto legal no debe implicar problemas, sino todo lo contrario; debe dar garantías adicionales en materia de seguridad de la información a las empresas que aplican los procesos de conformidad, así como ventajas competitivas que no deben ser desaprovechadas.

Análisis de la legislación comparada de (España).

Mediante esta legislación se dice que en España existe un marco legal de obligado cumplimiento, referente a las empresas y trabajadores en la cual tienen la obligación de velar por la protección de los datos de carácter personal, donde se describen la necesidad de proteger la privacidad de las personas, así como de datos especialmente protegidos y por lo cual deben dar garantías adicionales en materia de seguridad de la información a las diferentes empresas que se aplica.

I.3.- **PLANTEAMIENTO DEL PROBLEMA DE LA MONOGRAFÍA.**

- ¿Será que existe una normativa general y uniforme que regule la seguridad de nuestros datos que se encuentran depositados en la base de datos de la entidad pública?

- ¿Será de vital importancia para los ciudadanos, empresas y Estado esa información depositada en la base de datos de las entidad pública?

- ¿Estará protegida nuestra información que esta depositada en la base de datos de la entidad pública?

- ¿Qué mecanismos utilizan para proteger nuestra información?

- ¿Estará legislada la protección de nuestra información?

- ¿De qué manera podrá el estado garantizar la seguridad de la información depositada en la base de datos de la entidad pública?

CAPITULO II

FUNDAMENTOS TEORICOS, CONCEPTUALES Y TECNICAS DE LA SEGURIDAD INFORMATICA Y SU IMPLEMENTACION.

II.1.- SEGURIDAD INFORMATICA.

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Este problema será solucionado satisfaciendo las necesidades de comprensión del concepto "Seguridad" y "Sistema Informático" en torno de alguien (organización o particular) que gestiona información. Para esto es necesario acoplar los principios de Seguridad expuestos en un contexto informático y viceversa. En definitiva los expertos en seguridad y los expertos en informática deben interactuar interdisciplinariamente para que exista Seguridad Informática.

En el presente, cada vez que se mencione Información se estará haciendo referencia a la Información que es procesada por un Sistema Informático; definiendo este último como el "conjunto formado por las personas, computadoras (hardware y software), papeles, medios de almacenamiento digital, el entorno donde actúan y sus interacciones.".

"El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales), Control y Autenticidad de la información manejada por computadora."

II.1.1.- ANÁLISIS DEL O BJETIVO DE LA SEGURIDAD INFORMÁTICA.

Para comenzar el análisis de la Seguridad Informática se deberá conocer las características de lo que se pretende proteger: la Información así, definimos Dato como "la unidad mínima con la que compone cierta información. Datum es una palabra latina, que significa "lo que se da".

La Información "es una agregación de datos que tiene un significado específico más allá de cada uno de éstos", y tendrá un sentido particular según como y quien la procese, Ejemplo: 1, 9, 8 y 7 son datos; su agregación 1987 es Información.

Existe Información que debe o puede ser pública: puede ser visualizada por cualquier persona (por ejemplo índice de analfabetismo en un país); y aquella que debe ser privada: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos). En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo reconociendo las siguientes características en la Información:

1. Es Crítica: es indispensable para garantizar la continuidad operativa.
2. Es Valiosa: es un activo con valor en sí misma.
3. Es Sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

La **Integridad** de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

El **Control** sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.

La **Autenticidad** permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- **Protección a la Réplica:** mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.
- **No Repudio:** mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.
- **Consistencia:** se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- **Aislamiento:** este aspecto, íntimamente relacionado con la Confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.
- **Auditoria:** es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuándo las realiza.

Cabe definir **Amenaza**, en el entorno informático, como cualquier elemento que comprometa al sistema.

Gráfico 1 – Amenazas para la Seguridad

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

a. **La Prevención (antes):** mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.
b. **La Detección (durante):** mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.
c. **La Recuperación (después):** mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (Backuc) realizadas.

Luego el **Daño** es el resultado de la amenaza; aunque esto es sólo la mitad del axioma.
El daño también es el resultado de la no–acción, o acción defectuosa, del protector. El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y si lo hizo, se impusieron criterios comerciales por encima de los de seguridad. De allí que se deriven responsabilidades para la amenaza.

Luego, el protector será el encargado de detectar cada una de las Vulnerabilidades (debilidades) del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo. También será el encargado de aplicar las Contramedidas (técnicas de protección) adecuadas.

La Seguridad indicara el índice en que un Sistema de seguridad Informática está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir (según los especialistas imposible) en un 100% por lo que sólo se habla de Fiabilidad y se la define como "la probabilidad de que un sistema se comporte tal y como se espera de él" y se habla de Sistema Fiable en vez de sistema seguro.

Es importante remarcar que no existe el 100% de seguridad esperado o deseable en estas circunstancias (por ejemplo: al cruzar la calle ¿estamos 100% seguros que nada nos pasará?).

II.1.2. SISTEMA DE SEGURIDAD.

En los siguientes capítulos se estudiarán las distintas funciones que se deben asegurar en un sistema de informática.

I. **Reconocimiento**: cada usuario deberá identificarse al usar el sistema y cada operación del mismo será registrada con esta identificación. En este proceso se quiere conseguir que no se produzca un acceso y/o manipulación indebida de los datos o que en su defecto, esta quede registrada.
2. **Integridad**: un sistema integro es aquel en el que todas las partes que lo constituyen funcionan en forma correcta y en su totalidad.
3. **Aislamiento:** los datos utilizados por un usuario deben ser independientes de los de otro física y lógicamente (usando técnicas de ocultación y/o

compartimiento). También se debe lograr independencia entre los datos accesibles y los considerados críticos.

4. **Controlabilidad**: todos los sistemas y subsistemas deben estar bajo control permanente.
5. **Recuperabilidad**: en caso de emergencia, debe existir la posibilidad de recuperar los recursos perdidos o dañados.
6. **Administración y Custodia:** la vigilancia nos permitirá conocer, en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una realimentación del sistema de seguridad, de forma tal de mantenerlo actualizado contra nuevas amenazas.

II.1.3. DE QUIEN DEBEMOS PROTEGERNOS.

Se llama Intruso o Atacante a la persona que accede (o intenta acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no.

Ante la pregunta de los tipos de intrusos existentes actualmente, Julio C. Ardita Contesta lo siguiente:

"Los tipos de Intrusos podríamos caracterizarlos desde el punto de vista del nivel de conocimiento, formando una pirámide.

1. **Clase A:** el 80% en la base son los nuevos intrusos que bajan programas de Internet y prueban, están jugando son pequeños grupitos que se juntan y dicen vamos a probar.
2. **Clase B:** es el 12% son más peligroso, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo que está usando la víctima, testean las vulnerabilidades del mismo e ingresan por ellas.

3. **Clase C:** es el 5%. Es gente que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.
4. **Clase D:** el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

Para llegar desde la base hasta el último nivel se tarda desde 4 a 6 años, por el nivel de conocimiento que se requiere asimilar. Es práctica, conocer, programar, mucha tarea y mucho trabajo".

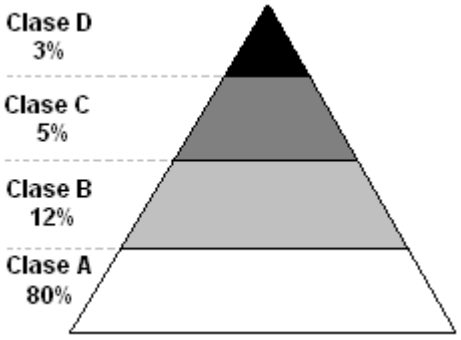


Gráfico 2 – Tipos de Intrusos. Fuente: CybSec S.A. http://www.cybsec.com

II.1.4. QUÉ DEBEMOS PROTEGER.

En cualquier sistema de informática existen tres elementos básicos a proteger: **el hardware, el software y los datos.**

Hardware entendemos el conjunto de todos los sistemas físicos del sistema informático: CPU, cableado, impresoras, CD–ROM, cintas, componentes de comunicación.

Software son todos los elementos lógicos que hacen funcional al hardware: sistema operativo, aplicaciones, utilidades.

Datos conjunto de información lógica que maneja el software y el hardware: bases de datos, documentos, archivos.

Para cualquiera de los elementos descriptos existen multitud de amenazas y ataques que se los puede clasificar en:

- **Ataques Pasivos**: el atacante no altera la comunicación, sino que únicamente la "escucha" o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico.

- **Ataques Activos**: estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cuatro categorías:

  - **Interrupción:** si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.

  - **Intercepción:** si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.

  - **Modificación:** si además de conseguir el acceso consigue modificar el objeto.
  - **Fabricación:** se consigue un objeto similar al original atacado de forma que es difícil distinguirlos entre sí.

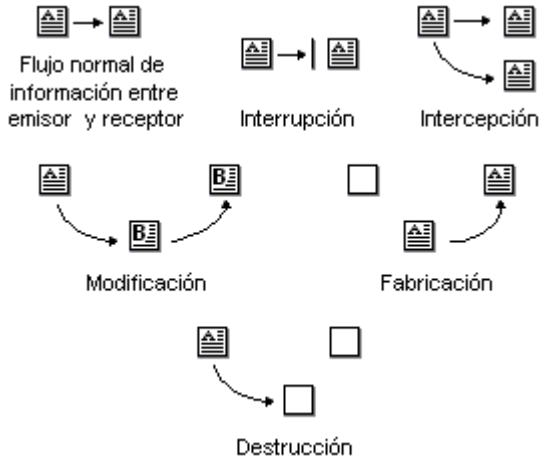


Gráfico 3 – Tipos de Ataques Activos. Fuentes: *http://www.cert.org*.

Con demasiada frecuencia se cree que los piratas son los únicos que amenazan nuestro sistema, siendo pocos los administradores que consideran todos los demás riesgos analizados en el presente.

II.1.5. RELACIÓN OPERATIVIDAD–SEGURIDAD.

Seleccionar las medidas de seguridad a implantar requiere considerar el equilibrio entre los intereses referidos a la seguridad, los requerimientos operacionales y la "amigabilidad" para el usuario.

Para ilustrar lo antes dicho imaginemos una computadora “extremadamente” segura:

- Instalada a 20 metros bajo tierra en un recinto de hormigón.
- Aislada informáticamente de otras computadoras.
- Aislada eléctricamente y alimentada por un sistema autónomo de triple reemplazo. Ahora imaginemos la utilidad de está “súper segura”

computadora: tendiente a nula.

Con esto refleja que la Seguridad y la Utilidad de una computadora son inversamente proporcionales; es decir que incrementar la seguridad en un sistema de informática, su operatividad desciende y viceversa.

$$Operatividad \propto \frac{1}{Seguridad}$$

Como se observa en el gráfico esta función se vuelve exponencial al acercarse al 100% de seguridad. Los costos se disparan (tendientes al infinito) por los complejos estudios que se deberán realizar para mantener este grado de seguridad.

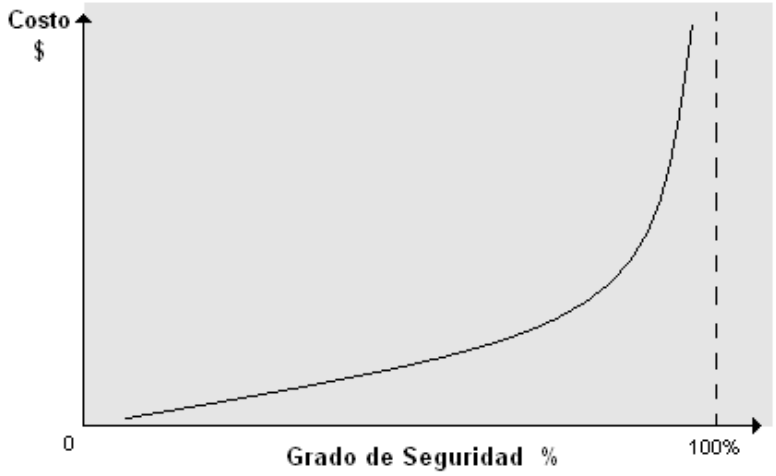


Gráfico 4 – Relación Operatividad–Seguridad. Fuente: ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1° Edición. Argentina. 1997. Página 26

Más allá al tratarse de una ciencia social, no determinística, se mantendrá la incertidumbre propia del comportamiento humano, que puede permitir a un atacante

violar el sistema, haciendo que los costos hayan sido, si bien no inútiles, excesivos.

Para ubicarnos en la vida real, veamos los datos obtenidos en marzo de 2009 por la consultora Ernst & Young [1] sobre 273 empresas de distintos sectores de actividad y países.

- El 40% de las empresas estudiadas consideran como un problema grave la seguridad informática.
- El "gasto" en Seguridad Informática oscila entre el 4% y el 10% del gasto total informático.
- El 83% de las empresas reconoce no haber emprendido nunca acciones legales después de un ataque.
- El 79% cree que existen mayores probabilidades de sufrir un ataque informático procedente del exterior. Esto, como se verá posteriormente es un error.
- El 66% consideran a la Seguridad y Privacidad de la información el impedimento principal para el crecimiento del comercio.
- Sólo el 39% hace uso de software estándar de seguridad y el 20% de este total hace uso avanzado de estas herramientas.

II.2.- SEGURIDAD FÍSICA.

Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

"Osorio Manuel Diccionario de Ciencias Jurídicas, Políticas y Sociales" Editorial Eliasta 2004

II.2.1. TIPOS DE DESASTRES.

No será la primera vez que se mencione en este trabajo, que cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este concepto vale, también, para el edificio en el que nos encontramos. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos. Para ejemplificar esto: valdrá de poco tener en cuenta aquí, en Santa Cruz, técnicas de seguridad ante terremotos, u otros; pero sí será de máxima utilidad en Los Ángeles, EE.UU.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara. A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

II.2.2.- INCENDIOS.

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Desgraciadamente los sistemas anti fuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputos.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

1. El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
2. El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
3. Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
4. Debe construirse un "falso piso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
5. Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.

Agencia Española de protección de datos legislación estatal.

II.2.3.- SEGURIDAD DEL EQUIPAMIENTO.

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

De todo lo anterior mencionado se recomienda:

El personal designado para usar extinguidores de fuego debe ser entrenado en su uso. Si hay sistemas de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con este proceso automático.

Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes.

Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y

requiere una lenta y costosa operación de limpieza.
Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel. Suministrar información, del centro de cómputo, al departamento local de bomberos, antes de que ellos sean llamados en una emergencia. Hacer que este departamento esté consciente de las particularidades y vulnerabilidades del sistema, por excesivas cantidades de agua y la conveniencia de una salida para el humo, es importante. Además, ellos pueden ofrecer excelentes consejos como precauciones para prevenir incendios.

II.2.4.- INUNDACIONES.

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

II.2.5.- CONDICIONES CLIMATOLÓGICAS.

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

II.2.6.- TERREMOTOS.

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros.

II.2.7.- R OBO.

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

II.2.8.- F RAUDE.

Cada año, millones de dólares son sustraídos de empresas y en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones

II.2.9.- SABOTAJE.

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos. Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

II.2.10.- CONTROL DE ACCESOS.

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

II.2.11.- CONTROL DE PERSONAS.

El Servicio de Vigilancia es el encargado del control de acceso de todas las personas al edificio. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

A cualquier personal ajeno a la planta se le solicitará completar un formulario de datos personales, los motivos de la visita, hora de ingreso y de salida, etc.
El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y salida del personal a los distintos sectores de la empresa.

En este caso la persona se identifica por algo que posee, por ejemplo una tarjeta de identificación. Cada una de ellas tiene un PIN (Personal Identificación Numero) único, siendo este el que se almacena en una base de datos para su posterior seguimiento, si fuera necesario.

Su mayor desventaja es que estas tarjetas pueden ser copiadas, robadas, etc. Permitiendo ingresar a cualquier persona que la posea.

Estas credenciales se pueden clasificar de la siguiente manera:

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

Las personas también pueden acceder mediante algo que saben (por ejemplo un número de identificación o un password) que se solicitará a su ingreso. Al igual que el caso de las tarjetas de identificación los datos ingresados se contrastarán contra una base donde se almacena los datos de las personas autorizadas. Este sistema tiene la desventaja que generalmente se eligen identificaciones sencillas, bien se olvidan dichas identificaciones o incluso las bases de datos pueden verse alteradas o robadas por personas no autorizadas.

II.2.12.- CONTROL DE VEHÍCULOS.

Para controlar el ingreso y salida de vehículos, el personal de vigilancia debe asentar en una planilla los datos personales de los ocupantes del vehículo, la marca y patente del mismo, y la hora de ingreso y salida de la empresa.

II.213.- UTILIZACIÓN DE DETECTORES DE METALES.

El detector de metales es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el detector, es regulable permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activará la alarma.

La utilización de este tipo de detectores debe hacerse conocer a todo el personal. De este modo, actuará como elemento disuasivo.

II.2.14.- UTILIZACIÓN DE SISTEMAS BIOMÉTRICOS.

Definimos a la Biometría como "la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos".

La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas, la forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).

II.2.15.- HUELLA DIGITAL.

Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados.
Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen más de ocho minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable.

II.2.16.- VERIFICACIÓN AUTOMÁTICA DE FIRMAS (VAF).

En este caso lo que se considera es lo que el usuario es capaz de hacer, aunque también podría encuadrarse dentro de las verificaciones biométricas, mientras es posible para un falsificador producir una buena copia visual.

La V.A.F. Usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada.

El equipamiento de colección de firmas es inherentemente de bajo costo y robusto. Esencialmente, consta de un bloque de metal (o algún otro material con propiedades acústicas similares) y una computadora barata.

II.2.17.- PROTECCIÓN ELECTRÓNICA.

Se llama así a la detección de robo, instrucción, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

II.2.18.- DETECTOR ULTRASÓNICO.

Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generará una perturbación en dicho campo que accionará la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas. La cobertura de este sistema puede llegar a un máximo de 40 metros cuadrados.

II.2.19.- CIRCUITOS CERRADOS DE TELEVISIÓN.

Permite el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizada como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

Todos los elementos anteriormente descriptos poseen un control contra sabotaje, de manera que si en algún momento se corta la alimentación o se produce la rotura de alguno de sus componentes, se enviará una señal a la central de alarma para que ésta accione los elementos de señalización correspondientes.

II.2.20.- EDIFICIOS INTELIGENTES.

La infraestructura inmobiliaria no podía quedarse rezagada en lo que se refiere a avances tecnológicos. Edificio Inteligente (surgido hace unos 10 años) se define como una estructura que facilita a usuarios y administradores, herramientas y servicios integrados a la administración y comunicación. Este concepto propone la integración de todos los sistemas existentes dentro del edificio, tales como teléfonos, comunicaciones por computadora, seguridad, control de todos los subsistemas del edificio (gas, calefacción, ventilación y aire acondicionado, etc.) y todas las formas de administración de energía.

Una característica común de los Edificios Inteligentes es la flexibilidad que deben tener para asumir modificaciones de manera conveniente y económica.

II.3.- SEGURIDAD LÓGICA.-

Luego de ver como nuestro sistema puede verse afectado por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

O.I.T. Seguridad Informatica: un nuevo consenso capítulo IV igualdad de género, informe de la comisión de la seguridad Informática.

Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

II.3.1. CONTROLES DE ACCESO.

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en base de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el National Institute for Standars and Technology (NIST) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema.

II.3.2.- ROLES.

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

II.3.3.- TRANSACCIONES.

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

II.3.4.- LIMITACIONES A LOS SERVICIOS.

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

II.3.5.- MODALIDAD DE ACCESO.

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- **Lectura**: el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- **Escritura**: este tipo de acceso permite agregar datos, modificar o borrar información.
- **Ejecución**: este acceso otorga al usuario el privilegio de ejecutar programas.
- **Borrado**: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.

II.3.6.- UBICACIÓN Y HORARIO.

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

II.3.7.- ENCRIPTACIÓN.

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso. Este tema será abordado con profundidad en el Capítulo sobre Protección del presente.

II.3.8.- LISTAS DE CONTROL DE ACCESOS.

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

II.3.9.- LÍMITES SOBRE LA INTERFASE DE USUARIO.

Esto límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interface de usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

II.3.10.- ETIQUETAS DE SEGURIDAD.

Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

II.3.11.- DISPOSITIVOS DE CONTROL DE PUERTOS.

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

II.3.12.- FIREWALLS O PUERTOS DE SEGURIDAD.

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Este tema será abordado con posterioridad.

II.3.13.- NIVELES DE SEGURIDAD INFORMÁTICA.

El estándar de niveles de seguridad más utilizado internacionalmente es el TCSEC Orange Book, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos. Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el nivel A, B1, B2, B3, C1 y C2.

II.3.13.1.- NIVEL A: PROTECCIÓN VERIFICADA.

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.
Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

II.3.13.2.- NIVEL B1: SEGURIDAD ETIQUETADA.

Este nivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto reservado, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

II.3.13.3.- NIVEL B2: PROTECCIÓN ESTRUCTURADA.

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

II.3.13.4.- NIVEL B3: DOMINIOS DE SEGURIDAD.

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad.

Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.

II.3.13.5.- NIVEL C1: PROTECCIÓN DISCRECIONAL.

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.
Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "súper usuario"; quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- **Acceso de control discrecional**: distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.
- **Identificación y Autentificación**: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

II.3.13.6.- NIVEL C2: PROTECCIÓN DE ACCESO CONTROLADO.

Este nivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

II.4.- PROTECCIÓN.

Una vez conocidas las vulnerabilidades y ataques a las que está expuesto un sistema es necesario conocer los recursos disponibles para protegerlo. Mientras algunas técnicas son evidentes (seguridad física por ejemplo) otras pautas no lo son tanto e incluso algunas pueden ocasionar una sensación de falsa seguridad.

Muchas de las vulnerabilidades estudiadas son el resultado de implementación incorrecta de tecnologías, otras son consecuencias de la falta de planeamiento de las mismas pero, como ya se ha mencionado, la mayoría de los agujeros de seguridad son ocasionados por los usuarios de dichos sistemas y es responsabilidad del administrador detectarlos y encontrar la mejor manera de cerrarlos.

En el presente capítulo, después de lo expuesto y vistas la gran cantidad de herramientas con las que cuenta el intruso, es el turno de estudiar implementaciones en la búsqueda de mantener el sistema seguro. Siendo reiterativo, ninguna de las técnicas expuestas a continuación representará el 100% de la seguridad deseado.

II.4.1. VULNERAR PARA PROTEGER.

Los intrusos utilizan diversas técnicas para quebrar los sistemas de seguridad de una red. Básicamente buscan los puntos débiles del sistema para poder colarse en ella. El trabajo de los Administradores y Tester no difiere mucho de esto. En lo que sí se diferencia, y por completo, es en los objetivos: mientras que un intruso penetra en las redes para distintos fines (investigación, daño, robo, etc.) un administrador lo hace para poder mejorar los sistemas de seguridad.

En palabras de Julio C. Ardita "los intrusos cuentan con grandes herramientas como los Scanner, los cracking de passwords, software de análisis de vulnerabilidades y los exploits" un administrador cuenta con todas ellas empleadas para bien, los sistemas de detección de intrusos y los sistemas de rastreo de intrusiones".

Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se lo conoce como Penetration Testing, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces.

El software y el Hardware utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina "políticas de seguridad internas" que cada organización (y usuario) debe generar e implementar.

II.4.2.- ADMINISTRACIÓN DE LA SEGURIDAD.

Es posible dividir las tareas de administración de seguridad en tres grandes grupos:

- **Autenticación:** se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.
- **Autorización: es** el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.
- **Auditoría:** se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su "voluntad de hacer algo" que permita detener un posible ataque antes de que éste suceda. A continuación se citan algunos de los métodos de protección más comúnmente empleados.

1. **Sistemas de detección de intrusos:** son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.
2. **Sistemas orientados a conexión de red:** monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de

efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuegos (Firewalls) y los Wrappers.

3. **Sistemas de análisis de vulnerabilidades:** analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La "desventaja" de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.
4. **Sistemas de protección a la integridad de información:** sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest (MD5) o bien sistemas que utilizan varios de ellos como PGP, Tripwire y DozeCrypt.
5. **Sistemas de protección a la privacidad de la información:** herramientas que utilizan criptografía para asegurar que la información sólo sea visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas se pueden citar a Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los Certificados Digitales.

Resumiendo, un modelo de seguridad debe estar formado por múltiples componentes o capas que pueden ser incorporadas de manera progresiva al modelo global de seguridad en la organización, logrando así el método más efectivo para disuadir el uso no autorizado de sistemas y servicios de red. Podemos considerar que estas capas son:

1. Política de seguridad de la organización.
2. Auditoría.
3. Sistemas de seguridad a nivel de Router–Firewall.

4. Sistemas de detección de intrusos.
5. Plan de respuesta a incidentes.
6. Penetratión Test.

II.4.3.- PENETRATION TEST, ETHICAL O PRUEBA DE VULNERABILIDAD.-

"El Penetration Test es un conjunto de metodologías y técnicas, para realizar una evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso, a cualquier entorno informático, de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como remotos."

El objetivo general del Penetration Test es acceder a los equipos informáticos de la organización tratada e intentar obtener los privilegios del administrador del sistema, logrando así realizar cualquier tarea sobre dichos equipos. También se podrá definir otros objetivos secundarios que permitan realizar pruebas puntuales sobre algunos ámbitos particulares de la empresa.

El Penetratión Test se compone de dos grandes fases de testeo:

- **Penetration Test Externo:** el objetivo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema. Se realizan desde fuera del Firewall.

  Consisten en penetrar la Zona Desmilitarizada para luego acceder a la red interna. Se compone de un elevado número de pruebas, entre las que se puede nombrar:

- Pruebas de usuarios y la "fuerza" de sus passwords.
- Captura de tráfico.
- Detección de conexiones externas y sus rangos de direcciones.

- Detección de protocolos utilizados.
- Scanning de puertos TCP, UDP e ICMP.
- Intentos de acceso vía accesos remotos, módems, Internet, etc.
- Análisis de la seguridad de las conexiones con proveedores, trabajadores remotos o entidades externas a la organización .
- Prueba de ataques de Denegación de Servicio.
- **Penetration Test Interno:** este tipo de testeo trata de demostrar cuál es el nivel de seguridad interno. Se deberá establecer que puede hacer un Insider y hasta donde será capaz de penetrar en el sistema siendo un usuario con privilegios bajos. Este Test también se compone de numerosas pruebas:
- Análisis de protocolos internos y sus vulnerabilidades.
- Autenticación de usuarios.
- Verificación de permisos y recursos compartidos.
- Test de los servidores principales (WWW, DNS, FTP, SMTP, etc.).
- Test de vulnerabilidad sobre las aplicaciones propietarias.
- Nivel de detección de la intrusión de los sistemas.
- Análisis de la seguridad de las estaciones de trabajo.
- Seguridad de la red.
- Verificación de reglas de acceso.
- Ataques de Denegación de Servicio

II.4.4. - HONEYPOTS–HONEYNETS.

Estas “Trampas de Red” son sistemas que se activan con la finalidad específica de que los expertos en seguridad puedan observar en secreto la actividad de los Hackers/Crackers en su hábitat natural.

Actualmente un equipo de Honeynet trabaja en el desarrollo de un documento sobre la investigación y resultados de su trampa, la cual fue penetrada a la semana de ser activada (sin publicidad).

"Consiste en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos. Los Honeynets dan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos. Ellos juegan con los archivos y conversan animadamente entre ellos sobre todos los 'fascinantes programas' que encuentran, mientras el personal de seguridad observa con deleite cada movimiento que hacen", dijo Dan Adams. "Francamente, siento una combinación de sentimientos con respecto a espiar a la gente, aunque no sean buenas personas".

II.4.5.- FIREWALLS.

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

De hecho, los Firewalls no tienen nada que hacer contra técnicas como la Ingeniería Social y el ataque de Insiders.

Un **Firewall** es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

1. Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
2. Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

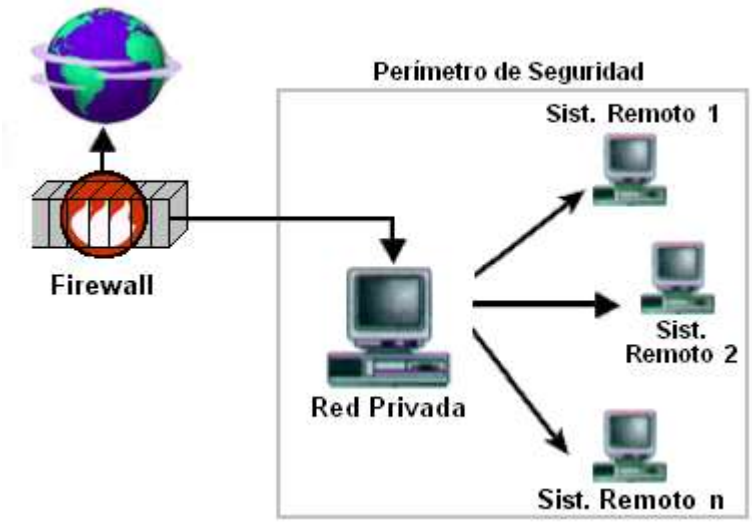


Gráfico 5 – Firewall

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación – des encriptación para entablar la comunicación.

II.4.6.- ROUTERS Y BRIDGES.

Cuando los paquetes de información viajan entre su destino y origen, vía TCP/IP, estos pasan por diferentes Routers (enrutadores a nivel de Red).

Los Routers son dispositivos electrónicos encargados de establecer comunicaciones

externas y de convertir los protocolos utilizados en protocolos de LAN y viceversa.

En cambio, si se conectan dos redes del tipo LAN se utilizan Bridges, los cuales son puentes que operan a nivel de Enlace.

La evolución tecnológica les ha permitido transformarse en computadoras muy especializadas capaz de determinar, si el paquete tiene un destino externo y el camino más corto y más descongestionado hacia el Routers de la red destino. En caso de que el paquete provenga de afuera, determina el destino en la red interna y lo deriva a la máquina correspondiente o devuelve el paquete a su origen en caso de que él no sea el destinatario del mismo.

Los Routers "toman decisiones" en base a un conjunto de datos, regla, filtros y excepciones que le indican que rutas son las más apropiadas para enviar los paquetes.

II.4.7.- BENEFICIOS DE UN FIREWALL.

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.

El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.

Otra causa que ha hecho que el uso de Firewalls se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten

direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados.

La limitación más grande que tiene un Firewall sencillamente es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje Back Doors, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall "no es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados.

Finalmente, un Firewall es vulnerable, él no protege de la gente que está dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna. Como moraleja: "cuanto mayor sea el tráfico de entrada y salida permitido por el Firewall, menor será la resistencia contra los paquetes externos. El único Firewall seguro (100%) es aquel que se mantiene apagado".

II.4.8.- DETECCIÓN DE INTRUSOS EN TIEMPO REAL.

La seguridad se tiene que tratar en conjunto. Este viejo criterio es el que recuerda que los sistemas de protección hasta aquí abordados, si bien son eficaces, distan mucho de ser la protección ideal.
Así, debe estar fuera de toda discusión la conveniencia de añadir elementos que controlen lo que ocurre dentro de la red (detrás de los Firewalls).

Como se ha visto, la integridad de un sistema se puede corromper de varias formas y la forma de evitar esto es con la instalación de sistemas de Detección de Intrusos en Tiempo Real, quienes:

- Inspeccionan el tráfico de la red buscando posibles ataques.
- Controlan el registro de los servidores para detectar acciones sospechosas (tanto de intrusos como de usuarios autorizados).
- Mantienen una base de datos con el estado exacto de cada uno de los archivos (Integrity Check) del sistema para detectar la modificación de los mismos.
- Controlan el ingreso de cada nuevo archivo al sistema para detectar Caballos de Troya o semejantes.
- Controlan el núcleo del Sistema Operativo para detectar posibles infiltraciones en él, con el fin de controlar los recursos y acciones del mismo.
- Avisan al administrador de cualquiera de las acciones mencionadas.

Cada una de estas herramientas permite mantener alejados a la gran mayoría de los intrusos normales. Algunos pocos, con suficientes conocimientos, experiencia y paciencia serán capaces de utilizar métodos sofisticados (u originales) como para voltear el perímetro de seguridad (interna + externa) y serán estos los casos que deban estudiarse para integrar a la política de seguridad existente mayor conocimiento y con él mayor seguridad.

CAPITULO III

POLÍTICAS DE SEGURIDAD

Hoy es imposible hablar de un sistema cien por cien seguros, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas.

La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios. “Si un Hacker quiere gastar cien mil dólares en equipos para descifrar una encriptación, lo puede hacer porque es imposible de controlarlo y en tratar de evitarlo se podrían gastar millones de dólares”.

La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

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

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

III.1.1.- POLÍTICAS DE SEGURIDAD INFORMÁTICA.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Esto adquiere mayor importancia aún cuando el tema abordado por estas políticas es la Seguridad Informática. Extensos manuales explicando cómo debe protegerse una computadora o una red con un simple Firewall, un programa antivirus o un monitor de sucesos. Falacias altamente remuneradas que ofrecen la mayor "Protección".

He intentado dejar en claro que la Seguridad Informática no tiene una solución definitiva aquí y ahora, sino que es y será (a mi entender) el resultado de la innovación tecnológica, a la par del avance tecnológico, por parte de aquellos que son los responsables de nuestros sistemas.
Es muy difícil armar algo global, por lo que siempre se trabaja en un plan de seguridad real, las políticas y procedimientos por un lado y la parte física por otra."

Para continuar, hará falta definir algunos conceptos:

Decisión: elección de un curso de acción determinado entre varios posibles.

Plan: conjunto de decisiones que definen cursos de acción futuros y los medios para conseguirlos. Consiste en diseñar un futuro deseado y la búsqueda del modo de conseguirlo.

Estrategia: conjunto de decisiones que se toman para determinar políticas, metas y programas.

Política: definiciones establecidas por la dirección, que determina criterios generales a adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.

Meta: objetivo cuantificado a valores predeterminados.

Procedimiento: Definición detallada de pasos a ejecutar para desarrollar una actividad determinada.

Norma: forma en que realiza un procedimiento o proceso.

Programa: Secuencia de acciones interrelacionadas y ordenadas en el tiempo que se utilizan para coordinar y controlar operaciones.

Proyección: predicción del comportamiento futuro, basándose en el pasado sin el agregado de apreciaciones subjetivas.

Pronóstico: predicción del comportamiento futuro, con el agregado de hechos concretos y conocidos que se prevé influirán en los acontecimientos futuros.

Control: capacidad de ejercer o dirigir una influencia sobre una situación dada o hecho. Es una acción tomada para hacer un hecho conforme a un plan.

Riesgo: proximidad o posibilidad de un daño, peligro. Cada uno de los imprevistos, hechos desafortunados, etc., que puede tener un efecto adverso. Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

Ahora, "una **Política de Seguridad** es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema."[2]

La RFC 1244 define **Política de Seguridad** como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán."

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; ante todo, una

---

O.I.T. Seguridad Social: Un nuevo consensó. Capítulo IV igualdad de género, informe de la comisión de la seguridad social, Conferencia Internacional del Trabajo, 89ava reunión 2001.

política de seguridad es una forma de comunicarse con los usuarios. Siempre hay que tener en cuenta que la seguridad comienza y termina con personas.”

- Ser holística (cubrir todos los aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a esta no se la ha cerrado con llave.
- Adecuarse a las necesidades y recursos. No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

Cualquier política de seguridad ha de contemplar los elementos claves de seguridad ya mencionados:

La Integridad, Disponibilidad, Privacidad y adicionalmente, Control, Autenticidad y Utilidad.

No debe tratarse de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el porqué de ello.

III.1.2.- EVALUACIÓN DE RIESGOS.

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas.

- Se debe poder obtener una evaluación económica del impacto de estos sucesos. Este valor se podrá utilizar para contrastar el costo de la protección de la información en análisis, versus el costo de volverla a producir (reproducir).
- Se debe tener en cuenta la probabilidad que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.
- Se debe conocer qué se quiere proteger, dónde y cómo, asegurando que con los costos en los que se incurren se obtengan beneficios efectivos. Para esto se deberá identificar los recursos (hardware, software, información, personal, accesorios, etc.) con que se cuenta y las amenazas a las que se está expuesto.

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización; pero se puede presuponer algunas preguntas que ayudan en la identificación de lo anteriormente expuesto.[3]

- "¿Qué puede ir mal?"
- "¿Con qué frecuencia puede ocurrir?"
- "¿Cuáles serían sus consecuencias?"
- "¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?"
- "¿Se está preparado para abrir las puertas del negocio sin sistemas, por un día, una semana, cuánto tiempo?"
- "¿Cuál es el costo de una hora sin procesar, un día, una semana...?"
- "¿Cuánto, tiempo se puede estar off–line sin que los clientes se vayan a la competencia?"
- "¿Se tiene forma de detectar a un empleado deshonesto en el sistema?"

"Ley 2298 de Ejecución Penal y Supervisión".

- “¿Se tiene control sobre las operaciones de los distintos sistemas?”
- “¿Cuantas personas dentro de la empresa, (sin considerar su honestidad), están en condiciones de inhibir el procesamiento de datos?”
- “¿A que se llama información confidencial y/o sensitiva?”
- “¿La información confidencial y sensitiva permanece así en los sistemas?”
- “¿La seguridad actual cubre los tipos de ataques existentes y está preparada para
- “¿Cuál es el costo de una hora sin procesar, un día, una semana...?”
- “¿Cuánto, tiempo se puede estar off–line sin que los clientes se vayan a la competencia?”
- “¿Se tiene forma de detectar a un empleado deshonesto en el sistema?”
- “¿Se tiene control sobre las operaciones de los distintos sistemas?”
- “¿Cuantas personas dentro de la empresa, (sin considerar su honestidad), están en condiciones de inhibir el procesamiento de datos?”
- “¿A que se llama información confidencial y/o sensitiva?”
- “¿La información confidencial y sensitiva permanece así en los sistemas?”
- “¿La seguridad actual cubre los tipos de ataques existentes y está preparada para adecuarse a los avances tecnológicos esperados?”
- “¿A quién se le permite usar que recurso?”
- “¿Quién es el propietario del recurso? y ¿quién es el usuario con mayores privilegios sobre ese recurso?”

Una vez obtenida la lista de cada uno de los riesgos se efectuará un resumen del tipo:

Tipo de Riesgo	Factor
Robo de hardware	Alto
Robo de información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus Informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

Tabla 6 – Tipo de Riesgo–Factor

Según esta tabla habrá que tomar las medidas pertinentes de seguridad para cada caso en particular, cuidando incurrir en los costos necesarios según el factor de riesgo representado.

III.1.3.- IDENTIFICACIÓN DE AMENAZA.

Una vez conocidos los riesgos, los recursos que se deben proteger y como su daño o falta pueden influir en la organización es necesario identificar cada una de las amenazas y vulnerabilidades que pueden causar estas bajas en los recursos. Como ya se mencionó existe una relación directa entre amenaza y vulnerabilidad a tal punto que si una no existe la otra tampoco.

Se suele dividir las amenazas existentes según su ámbito de acción:

- Desastre del entorno (Seguridad Física).
- Amenazas del sistema (Seguridad Lógica).

- Amenazas en la red (Comunicaciones).
- Amenazas de personas (Insiders–Outsiders).

Se debería disponer de una lista de amenazas (actualizadas) para ayudar a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar. Es importante que los Administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan de forma continua.

En la siguiente sección se explica una metodología para definir una estrategia de seguridad informática que se puede utilizar para implementar directivas y controles de seguridad con el objeto de aminorar los posibles ataques y amenazas. Los métodos se pueden utilizar en todos los tipos de ataques a sistemas, independientemente de que sean intencionados, no intencionados o desastres naturales.

La metodología se basa en los distintos ejemplos (uno para cada tipo de amenaza) y contempla como hubiera ayudado una política de seguridad en caso de haber existido.

III.1.4.- EVALUACIÓN DE COSTOS.

Desde un punto de vista oficial, el desafío de responder la pregunta del valor de la información ha sido siempre difícil, y más difícil aún hacer estos costos justificables, siguiendo el principio que "si desea justificarlo, debe darle un valor".[4]

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones.

Osorio Manuel "Diccionario de Ciencias Jurídicas, Políticas y Sociales" Editorial Eliasta 2004.

Reglamento de INESES. (Régimen de Corto Plazo).

Además, las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son reticentes a dedicar recursos a esta tarea. Por eso es importante entender que los esfuerzos invertidos en la seguridad son costeables.

La evaluación de costos más ampliamente aceptada consiste en cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades. Un planteamiento posible para desarrollar esta política es el análisis de lo siguiente:

- ¿Qué recursos se quieren proteger?
- ¿De qué personas necesita proteger los recursos?
- ¿Qué tan reales son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?

Con esas sencillas preguntas (más la evaluación de riesgo) se debería conocer cuáles recursos vale la pena (y justifican su costo) proteger, y entender que algunos son más importantes que otros.

El objetivo que se persigue es lograr que un ataque a los bienes sea más costoso que su valor, invirtiendo menos de lo que vale. Para esto se define tres costos fundamentales:

- **CP:** Valor de los bienes y recursos protegidos.
- **CR:** Costo de los medios necesarios para romper las medidas de seguridad establecidas.
- **CS:** Costo de las medidas de seguridad.

Para que la política de seguridad sea lógica y consistente se debe cumplir que:

- **CR > CP**: o sea que un ataque para obtener los bienes debe ser más costoso que el valor de los mismos. Los beneficios obtenidos de romper las medidas de seguridad
  no deben compensar el costo de desarrollo del ataque.
- **CP > CS:** o sea que el costo de los bienes protegidos debe ser mayor que el costo
  de la protección.
- "**Minimizar** el costo de la protección manteniéndolo por debajo del de los bienes protegidos". Si proteger los bienes es más caro de lo que valen (el lápiz dentro de
  la caja fuerte), entonces resulta más conveniente obtenerlos de nuevo en vez de protegerlo.
- "**Maximizar** el costo de los ataques manteniéndolo por encima del de los bienes protegidos"[5]. Si atacar el bien es más caro de lo que valen, al atacante le conviene más obtenerlo de otra forma menos costosa.

Se debe tratar de valorar los costos en que se puede incurrir en el peor de los casos contrastando con el costo de las medidas de seguridad adoptadas. Se debe poner especial énfasis en esta etapa para no incurrir en el error de no considerar costos, muchas veces, ocultos y no obvios (costos derivados).

III.1.5.- VALOR INTRÍNSECO.

Es el más fácil de calcular (pero no fácil) ya que solo consiste en otorgar un valor a la información contestando preguntas como las mencionadas y examinando minuciosamente todos los componentes a proteger.

---

http. // www.cybsec.com.

III.1.6.- COSTOS DERIVADOS DE LA PÉRDIDA.

Una vez más deben abarcarse todas las posibilidades, intentando descubrir todos los valores derivados de la pérdida de algún componente del sistema. Muchas veces se trata del valor añadido que gana un atacante y la repercusión de esa ganancia para el entorno, además del costo del elemento perdido. Deben considerarse elementos como:

- Información aparentemente inocua como datos personales, que pueden permitir a alguien suplantar identidades.

- Datos confidenciales de acuerdos y contratos que un atacante podría usar para su beneficio.

- Tiempos necesarios para obtener ciertos bienes. Un atacante podría acceder a ellos para ahorrarse el costo (y tiempo) necesario para su desarrollo.

III.1.7.- PUNTO DE EQUILIBRIO.

Una vez evaluados los riesgos y los costos en los que se está dispuesto a incurrir y decidido el nivel de seguridad a adoptar, podrá obtenerse un punto de equilibrio entres estas magnitudes:

Htto://www.agpl.es/ipload/canal documentación/estatal ley No. 2015.

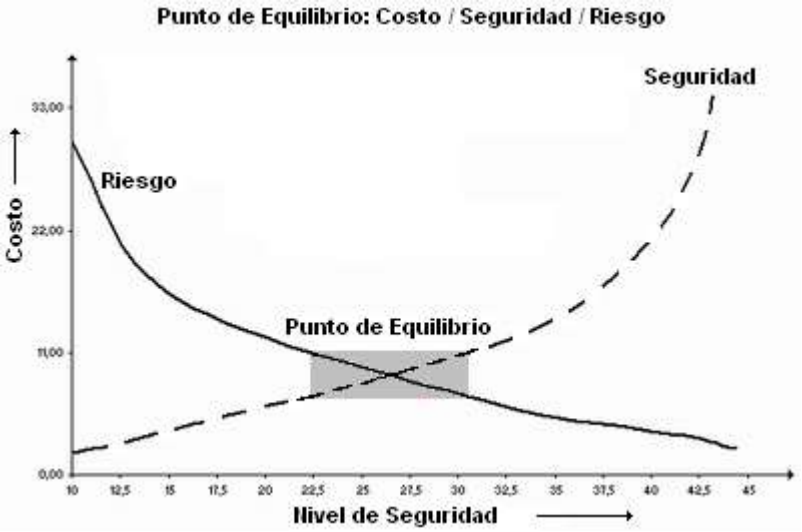


Gráfico 7 – Punto de equilibrio Costo/Seguridad

Como puede apreciarse los riesgos disminuyen al aumentar la seguridad (y los costos en los que incurre) pero como ya se sabe los costos tenderán al infinito sin lograr el 100% de seguridad y por supuesto nunca se logrará no correr algún tipo de riesgo. Lo importante es lograr conocer cuan seguro se estará conociendo los costos y los riesgos que se corren (Punto de Equilibrio).

III.2.- ESTRATEGIA DE SEGURIDAD.

Para establecer una estrategia adecuada es conveniente pensar una política de protección en los distintos niveles que esta debe abarcar y que no son ni más ni menos que los estudiados hasta aquí: Física, Lógica, Humana y la interacción que existe entre estos factores.

En cada caso considerado, el plan de seguridad debe incluir una estrategia Proactiva y otra Reactiva.[6]

---

http/www.monografia. Com. htm.

La **Estrategia Proactiva** (proteger y proceder) o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar esta estrategia.

La **Estrategia Reactiva** (perseguir y procesar) o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia Proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Con respecto a la postura que puede adoptarse ante los recursos compartidos:

- **Lo que no se permite expresamente está prohibido**: significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida.
- **Lo que no se prohíbe expresamente está permitido**: significa que, a menos que se indique expresamente que cierto servicio no está disponible, todos los demás sí lo estarán.

Estas posturas constituyen la base de todas las demás políticas de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir qué acciones se toleran y cuáles no.
Actualmente, y "gracias" a las, cada día más repetitivas y eficaces, acciones que atentan contra los sistemas informáticos los expertos se inclinan por recomendar la primera política mencionada.

III.2.1.- IMPLEMENTACIÓN.

La implementación de medidas de seguridad, es un proceso Técnico–Administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Se deberá tener en cuenta que la implementación de Políticas de Seguridad, trae aparejados varios tipos de problemas que afectan el funcionamiento de la organización. La implementación de un sistema de seguridad conlleva a incrementar la complejidad en la operatoria de la organización, tanto técnica como administrativamente.

Por esto, será necesario superar cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen.

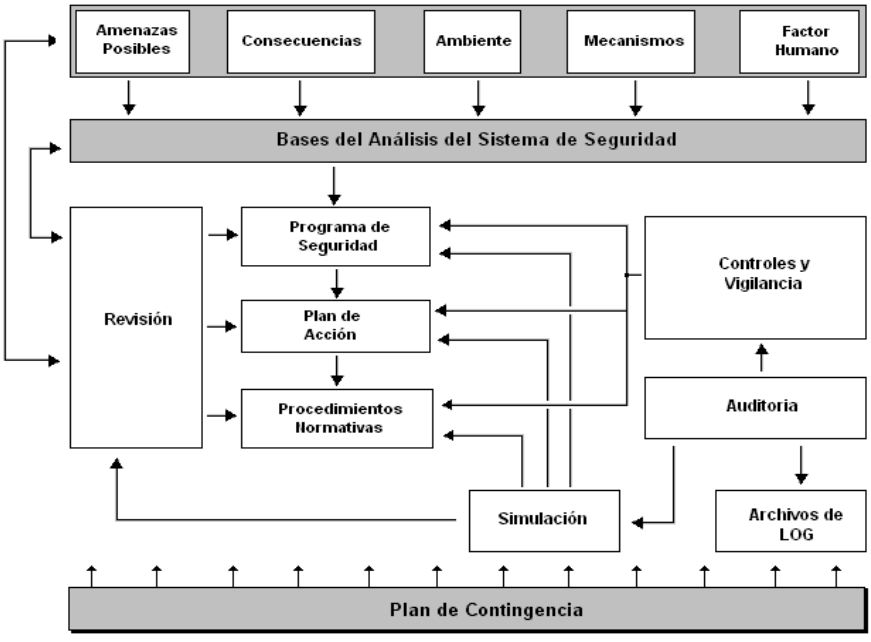
Es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración y deberá abarcar en lo siguiente.

- Alcance de la política, incluyendo sistemas y personal sobre el cual se aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidad de cada uno de los servicios, recurso y responsables en todos los niveles de la organización.
- Responsabilidades de los usuarios con respecto a la información que generan y a la que tienen acceso.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política.

- Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. Pero, no debe especificar con exactitud qué pasara o cuándo algo sucederá; ya que no es una sentencia obligatoria de la ley.
- Explicaciones comprensibles (libre de tecnicismos y términos legales pero sin sacrificar su precisión) sobre el porqué de las decisiones tomadas.
- Finalmente, como documento dinámico de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta y rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, etc.

Una proposición de una forma de realizar una PSI adecuada puede apreciarse en el siguiente diagrama:

Gráfico 8– Fuente: Manual de Seguridad en Redes. http://www.arcert.gov.ar



Se comienza realizando una evaluación del factor humano, el medio en donde se desempeña, los mecanismos con los cuales se cuenta para llevar a cabo la tarea encomendada, las amenazas posibles y sus posibles consecuencias.

Luego de evaluar estos elementos y establecida la base del análisis, se originan un programa de seguridad, el plan de acción y las normas y procedimientos a llevar a cabo.

Para que todo lo anterior llegue a buen fin debe realizarse un control periódico de estas políticas, que asegure el fiel cumplimiento de todos los procedimientos enumerados. Para asegurar un marco efectivo se realiza una auditoría a los archivos Logs de estos controles.

Con el objeto de confirmar que todo lo creado funciona en un marco real, se realiza una simulación de eventos y acontecimientos que atenten contra la seguridad del sistema. Esta simulación y los casos reales registrados generan una realimentación y revisión que permiten adecuar las políticas generadas en primera instancia.

Por último el Plan de Contingencia es el encargado de suministrar el respaldo necesario en caso en que la política falle.

Es importante destacar que la Seguridad debe ser considerada desde la fase de diseño de un sistema. Si la seguridad es contemplada luego de la implementación del mismo, el personal se enfrentará con problemas técnicos, humanos y administrativos muchos mayores que implicaran mayores costos para lograr, en la mayoría de los casos, un menor grado de seguridad.

---

http:/www.hispasec.com./corporate.

"Construya la seguridad desde el principio. La máxima de que es más caro añadir después de la implementación es cierta." [7] Julio C. Ardita menciona: "Muchas veces nos llaman cuando está todo listo, faltan dos semanas y quieren que lo aseguremos, llegamos, miramos y vemos que la seguridad es imposible de implementar. Últimamente nos llaman en el diseño y nosotros los orientamos y proponemos las soluciones que se pueden adoptar" [8]Queda claro que este proceso es dinámico y continuo, sobre el que hay que adecuarse continuamente a fin de subsanar inmediatamente cualquier debilidad descubierta**,** con el fin de que estas políticas no caigan en desuso.

III.2.2.- AUDITORÍA Y CONTROL.

Se considera que la Auditoría son los "ojos y oídos" de la dirección, que generalmente no puede, no sabe o no debe realizar las verificaciones y evaluaciones.

La Auditoría consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno y cuando lo hace.

En cuanto al objetivo del Control es contrastar el resultado final obtenido contra el deseado a fin de incorporar las correcciones necesarias para alcanzarlo, o bien verificar la efectividad de lo obtenido.

El concepto de auditoría es mucho más que esto. Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.

---

http.//www.cybsec.com.

La palabra auditoria proviene del latín *auditorius,* de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír.
En un principio esta definición carece de la explicación del objetivo fundamental que persigue todo auditor: evaluar la eficiencia y eficacia.
"La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevado a cabo son de carácter indudable."

De todo esto sacamos como deducción que la auditoría es un examen crítico pero no mecánico, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

Los principales objetivos que constituyen a la auditoría Informática son el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

El auditor informático ha de velar por la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz Sistema de Información. Claro está, que para la realización de una auditoría informática eficaz, se debe entender a la empresa en su más amplio sentido, ya que una Universidad, un Ministerio o un Hospital son tan empresas como una Sociedad Anónima o empresa Pública. Todos utilizan la informática para gestionar sus "negocios" de forma rápida y eficiente con el fin de obtener beneficios económicos y de costes.
Por eso, al igual que los demás órganos de la empresa (Balances y Cuentas de Resultados, Tarifas, Sueldos, etc.), los Sistemas Informáticos están sometidos al control

correspondiente, o al menos debería estarlo. La importancia de llevar un control de esta herramienta se puede deducir de varios aspectos. He aquí algunos:

- Las computadoras y los Centros de Proceso de Datos se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia y el terrorismo. En este caso interviene la Auditoría Informática de Seguridad.
- Las computadoras creadas para procesar y difundir resultados o información elaborada pueden producir resultados o información errónea si dichos datos son, a su vez, erróneos. Este concepto obvio es a veces olvidado por las mismas empresas que terminan perdiendo de vista la naturaleza y calidad de los datos de entrada a sus Sistemas Informáticos, con la posibilidad de que se provoque un efecto cascada y afecte a Aplicaciones independientes. En este caso interviene la Auditoría Informática de Datos.
- Un Sistema Informático mal diseñado puede convertirse en una herramienta harto peligrosa para la empresa: como las maquinas obedecen ciegamente a las órdenes recibidas y la modelización de la empresa está determinada por las computadoras que materializan los Sistemas de Información, la gestión y la organización de la empresa no puede depender de un Software y Hardware mal diseñados.

Estos son solo algunos de los varios inconvenientes que puede presentar un Sistema Informático, por eso, la necesidad de la Auditoría de Sistemas.

III.2.3.- AUDITORÍA.

La auditoria nace como un instrumento de control de algunas instituciones estatales y privadas. Su función inicial es estrictamente económico-financiero.

La función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones. Queda a cargo de la empresa tomar las decisiones pertinentes. La auditoría contiene elementos de análisis, verificación y exposición de

debilidades y disfunciones. Aunque pueden aparecer sugerencias, planes de acción para eliminar las disfunciones y debilidades antedichas; estas sugerencias plasmadas en el Informe final reciben el nombre de Recomendaciones.
Las funciones de análisis y revisión que el auditor informático realiza, puede chocar con la psicología del auditado, ya que es un informático y tiene la necesidad de realizar sus tareas con racionalidad y eficiencia.

El nivel técnico del auditor es a veces insuficiente, dada la gran complejidad de los Sistemas, unidos a los plazos demasiado breves de los que suelen disponer para realizar su tarea.

El auditor somete al sistema a una serie de cuestionarios. Dichos cuestionarios, llamados Check List, son guardados celosamente por las empresas auditoras, ya que son activos importantes de su actividad. Las Check List tienen que ser comprendidas por el auditor al pie de la letra, ya que si son mal aplicadas y mal recitadas se pueden llegar a obtener resultados distintos a los esperados por la empresa auditora. La Check List puede llegar a explicar cómo ocurren los hechos pero no por qué ocurren. El cuestionario debe estar subordinado a la regla, norma, método. Sólo una metodología precisa puede desentrañar las causas por las cuales se realizan actividades teóricamente inadecuadas o se omiten otras correctas.

El auditor sólo puede emitir un juicio global o parcial basado en hechos y situaciones incontrovertibles, careciendo de poder para modificar la situación analizada por él mismo.

III.2.3.1.- AUDITORÍA INTERNA Y AUDITORÍA EXTERNA.

La auditoría interna se realiza con recursos materiales, personas que pertenecen a la empresa auditada. Los empleados que realizan esta tarea son remunerados

económicamente. La auditoría interna existe por expresa decisión de la Empresa, o sea, que puede optar por su disolución en cualquier momento.

Por otro lado, la auditoría externa es realizada por personas afines a la empresa auditada; es siempre remunerada. Se presupone una mayor objetividad que en la Auditoría Interna, debido al mayor distanciamiento entre auditores y auditados.

La auditoría informática interna cuenta con algunas ventajas adicionales muy importantes respecto de la auditoría externa, las cuales no son tan perceptibles como en las auditorías convencionales. La auditoría interna tiene la ventaja de que puede actuar periódicamente realizando Revisiones globales, como parte de su Plan Anual y de su actividad normal. Los auditados conocen estos planes y se habitúan a las Auditorías, especialmente cuando las consecuencias de las Recomendaciones habidas benefician su trabajo.

En una empresa, los responsables de Informática escuchan, orientan e informan sobre las posibilidades técnicas y los costes de tal Sistema. Con voz, pero a menudo sin voto, Área informática trata de satisfacer lo más adecuadamente posible aquellas necesidades. La empresa necesita controlar su Informática y ésta necesita que su propia gestión esté sometida a los mismos Procedimientos y estándares que el resto de aquella. La conjunción de ambas necesidades cristaliza en la figura del auditor interno informático.

En cuanto a empresas se refiere, solamente las más grandes pueden poseer una Auditoría propia y permanente, mientras que el resto acuden a las auditorías externas.

Puede ser que algún profesional informático sea trasladado desde su puesto de trabajo a la Auditoría Interna de la empresa cuando ésta existe. Finalmente, la propia área informática requiere de su propio grupo de Control Interno, con implantación física en su estructura, puesto que si se ubicase dentro de la estructura Informática ya no sería independiente. Hoy, ya existen varias organizaciones Informáticas dentro de la misma

empresa, y con diverso grado de autonomía, que son coordinadas por órganos corporativos de Sistemas de Información de las Empresas.
Una Empresa o Institución que posee auditoría interna puede y debe en ocasiones contratar servicios de auditoría externa. Las razones para hacerlo suelen ser:

- Necesidad de auditar una materia de gran especialización, para la cual los servicios propios no están suficientemente capacitados.
- Contrastar algún Informe interno con el del externo, en aquellos supuestos de emisión interna de graves recomendaciones que chocan con la opinión generalizada de la propia empresa.
- Servir como mecanismo protector de posibles auditorías informáticas externas decretadas por la misma empresa.
- Aunque la auditoría interna sea independiente del Departamento de Sistemas, sigue siendo la misma empresa, por lo tanto, es necesario que se le realicen auditorías externas como para tener una visión desde afuera de la empresa.

La auditoría informática, tanto externa como interna, debe ser una actividad exenta de cualquier contenido o matiz "político" ajeno a la propia estrategia y política general de la empresa. La función auditora puede actuar de oficio o iniciativa del propio órgano, o a instancias de parte, esto es, por encargo de la dirección o cliente.

III.2.4.-ALCANCE DE LA AUDITORÍA INFORMÁTICA.

El alcance definirá con precisión el entorno y los límites de desarrollo de la auditoria informática, el alcance figurara expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas.

***Control de integridad de registros:**

Hay Aplicaciones que comparten registros, son registros comunes. Si una Aplicación no tiene integrado un registro común, cuando lo necesite utilizar no lo va encontrar y, por lo tanto, la aplicación no funcionaría como debería.

***Control de validación de errores:**

Se corrobora que el sistema que se aplica para detectar y corregir errores sea eficiente.

III.2.5.- CARACTERÍSTICAS DE LA AUDITORÍA INFORMÁTICA.

La información de la empresa es importante, se ha convertido en un Activo Real de la misma, como sus Stocks o materias primas. Por ende se deben realizar inversiones informáticas, materia de la que se ocupa la Auditoría de Inversión Informática.

Del mismo modo, los Sistemas Informáticos deben proteger de modo global y particular: a ello se debe la existencia de la Auditoría de Seguridad Informática en general, o la auditoría de Seguridad de alguna de sus áreas, como pudieran ser Desarrollo o Técnica de Sistemas.

Cuando se producen cambios estructurales en el Área Informática, se reorganiza de alguna forma su función: se está en el campo de la Auditoría de Organización Informática.

Estos tres tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoría parcial. De otra manera: cuando se realiza una auditoria del área de Desarrollo de Proyectos de la Informática de una empresa, es porque en ese Desarrollo existen, además de ineficiencias, debilidades de organización, inversiones, seguridad.

III.2.6.- SÍNTOMAS DE NECESIDAD DE UNA AUDITORÍA.

Las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en siguientes clases:

- Síntomas de descoordinación y desorganización:

- No coinciden los objetivos del Área Informática con los objetivos de la Empresa.

- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

[Puede ocurrir con algún cambio masivo de personal, una reestructuración fallida de alguna área o en la modificación de alguna Norma importante]

- Síntomas de mala imagen e insatisfacción de los usuarios:

- No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.

- No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.

- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

- Síntomas de debilidades económico-financiero:

- Incremento desmesurado de costes.

- Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).

- Desviaciones Presupuestarias significativas.

- Costes y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).

- Síntomas de Inseguridad: Evaluación de nivel de riesgos

- Seguridad Lógica

- Seguridad Física

- Confidencialidad

- Continuidad del Servicio. Es un concepto aún más importante que la Seguridad. Establece las estrategias de continuidad entre fallos mediante Planes de Contingencia*

Totales y Locales.

- Centro de Proceso de Datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoría. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

***Planes de Contingencia:**

Por ejemplo, la empresa sufre un corte total de energía o explota, ¿Cómo sigo operando en otro lugar? Lo que generalmente se pide es que se hagan Backup de la información diariamente y que aparte, sea doble, para tener un Backup en la empresa y otro afuera de ésta. Una empresa puede tener unas oficinas paralelas que posean servicios básicos (luz, teléfono, agua) distintos de los de la empresa principal, es decir, si a la empresa principal le proveía teléfono Telecom, a las oficinas paralelas, Telefónica. En este caso, si se produce la inoperancia de Sistemas en la empresa principal, se utilizaría el Backup para seguir operando en las oficinas paralelas. Los Backup se pueden acumular durante dos meses, o el tiempo que estipule la empresa, y después se van reciclando.

III.2.7.- OBJETIVOS FUNDAMENTALES DE LA AUDITORÍA INFORMÁTICA: OPERATIVIDAD.

La operatividad es una función consistente en que la organización y las maquinas funcionen, siquiera mínimamente. No es admisible detener la maquinaria informática para descubrir sus fallos y comenzar de nuevo. La auditoría debe iniciar su actividad cuando los Sistemas están operativos, es el principal objetivo el de mantener tal situación. Tal objetivo debe conseguirse tanto a nivel global como parcial.

La operatividad de los Sistemas ha de constituir entonces la principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de Controles Técnicos Generales de Operatividad y Controles Técnicos Específicos de Operatividad, previos a cualquier actividad de aquel.

- Los Controles Técnicos Generales son los que se realizan para verificar la compatibilidad de funcionamiento simultáneo del Sistema Operativo y el Software de base con todos los subsistemas existentes, así como la compatibilidad del Hardware y del Software instalados. Estos controles son importantes en las instalaciones que cuentan con varios competidores, debido a que la profusión de entornos de trabajo muy diferenciados obliga a la contratación de diversos productos de Software básico, con el consiguiente riesgo de abonar más de una vez el mismo producto o desaprovechar parte del Software abonado. Puede ocurrir también con los productos de Software básico desarrolla-dos por el personal de Sistemas Interno, sobre todo cuando los diversos equipos están ubicados en Centros de Proceso de Datos geográficamente alejados. Lo negativo de esta situación es que puede producir la inoperatividad del conjunto. Cada Centro de Proceso de Datos tal vez sea operativo trabajando independientemente, pero no será posible la interconexión e intercomunicación de todos los Centros de Proceso de Datos si no existen productos comunes y compatibles.
- Los Controles Técnicos Específicos, de modo menos acusado, son igualmente necesarios para lograr la Operatividad de los Sistemas. Un ejemplo de lo que se puede encontrar mal son parámetros de asignación automática de espacio en disco que dificulten o impidan su utilización posterior por una Sección distinta de la que lo generó. También, los periodos de retención de ficheros comunes a varias Aplicaciones pueden estar definidos con distintos plazos en cada una de ellas, de modo que la pérdida de información es un hecho que podrá producirse con facilidad, quedando inoperativa la explotación de alguna de las Aplicaciones mencionadas.

III.2.8.- REVISIÓN DE CONTROLES DE LA GESTIÓN INFORMÁTICA.

Una vez conseguida la Operatividad de los Sistemas, el segundo objetivo de la auditoría es la verificación de la observancia de las normas teóricamente existentes en el

departamento de Informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

1. Las Normas Generales de la Instalación Informática. Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa, y sobre todo verificando que esta Normativa General Informática no está en contradicción con alguna Norma General no informática de la empresa.
2. Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de Explotación. Tampoco el alta de una nueva Aplicación podría producirse si no existieran los Procedimientos de Backup y Recuperación correspondientes.
3. Los Procedimientos Específicos Informáticos. Igualmente, se revisara su existencia en las áreas fundamentales. Así, Explotación no debería explotar una Aplicación sin haber exigido a Desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los Procedimientos Específicos no se opongan a los Procedimientos Generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la Normativa y los Procedimientos Generales de la propia empresa, a los que la Informática debe estar sometida.

III.2.9.- AUDITORÍA INFORMÁTICA DE EXPLOTACIÓN.

La Explotación Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc. La explotación informática se puede considerar como una fabrica con ciertas peculiaridades que la distinguen de las reales. Para realizar la Explotación Informática se dispone de una materia prima, los datos, que sea necesario transformar, y que se sometan previamente a

controles de integridad y calidad. La transformación se realiza por medio del Proceso informático, el cual está gobernado por programas. Obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

Auditar Explotación consiste en auditar las secciones que la componen y sus interrelaciones. La Explotación Informática se divide en tres grandes áreas: Planificación, Producción y Soporte Técnico, en la que cada cual tiene varios grupos.

Control de Entrada de Datos:

Se analizará la captura de la información en soporte compatible con los Sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verificará que los controles de integridad y calidad de datos se realizan de acuerdo a Norma.

Planificación y Recepción de Aplicaciones:

Se auditarán las normas de entrega de Aplicaciones por parte de Desarrollo, verificando su cumplimiento y su calidad de interlocutor único. Deberán realizarse muestreos selectivos de la Documentación de las Aplicaciones explotadas. Se inquirirá sobre la anticipación de contactos con Desarrollo para la planificación a medio y largo plazo.

Centro de Control y Seguimiento de Trabajos:

Se analizará cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación Informática ejecuta procesos por cadenas o lotes sucesivos (Batch), o en tiempo real (Tiempo Real). Mientras que las Aplicaciones de Teleproceso están permanentemente activas y la función de Explotación se limita a vigilar y recuperar incidencias, el trabajo Batch absorbe una buena parte de los efectivos de Explotación. En muchos Centros de Proceso de Datos, éste órgano recibe el nombre de Centro de Control

de Batch. Este grupo determina el éxito de la explotación, en cuanto que es uno de los factores más importantes en el mantenimiento de la producción.

Operación. Salas de Ordenadores:

Se intentarán analizar las relaciones personales y la coherencia de cargos y salarios, así como la equidad en la asignación de turnos de trabajo. Se verificará la existencia de un responsable de Sala en cada turno de trabajo. Se analizará el grado de automatización de comandos, se verificara la existencia y grado de uso de los Manuales de Operación. Se analizará no solo la existencia de planes de formación, sino el cumplimiento de los mismos y el tiempo transcurrido para cada Operador desde el último Curso recibido. Se estudiarán los montajes diarios y por horas de cintas o cartuchos, así como los tiempos transcurridos entre la petición de montaje por parte del Sistema hasta el montaje real. Se verificarán las líneas de papel impresas diarias y por horas, así como la manipulación de papel que comportan.

Centro de Control de Red y Centro de Diagnosis:

El Centro de Control de Red suele ubicarse en el área de producción de Explotación. Sus funciones se refieren exclusivamente al ámbito de las Comunicaciones, estando muy relacionado con la organización de Software de Comunicaciones de Técnicas de Sistemas. Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos. Se verificará la existencia de un punto focal único, desde el cual sean perceptibles todos las líneas asociadas al Sistema. El Centro de Diagnosis es el ente en donde se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de Software como de Hardware. El Centro de Diagnosis está especialmente indicado para informáticos grandes y con usuarios dispersos en un amplio territorio. Es uno de los elementos que más contribuyen a configurar la imagen de la Informática de la empresa. Debe ser auditada desde esta perspectiva, desde la sensibilidad del usuario sobre el servicio que se le dispone. No basta con comprobar la

eficiencia técnica del Centro, es necesario analizarlo simultáneamente en el ámbito de Usuario.

III.2.10.- AUDITORÍA INFORMÁTICA DE DESARROLLO DE PROYECTOS O APLICACIONES.

La función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizarles tiene la empresa. Muy escuetamente, una Aplicación recorre las siguientes fases:

- Prerrequisitos del Usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (Pre programación y Programación)
- Pruebas
- Entrega a Explotación y alta para el Proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costes, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

Una auditoría de Aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

1. Revisión de las metodologías utilizadas: Se analizaran éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
2. Control Interno de las Aplicaciones: se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de Desarrollo.

3. Satisfacción de usuarios*:* Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó. La aquiescencia del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.
4. Control de Procesos y Ejecuciones de Programas Críticos*:* El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de Desarrollo de Aplicaciones. Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programa módulo no coincidieran se podría provocar, desde errores de bulto que producirían graves y altos costes de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc. Por ende, hay normas muy rígidas en cuanto a las Librerías de programas; aquellos programas fuente que hayan sido dados por bueno por Desarrollo, son entregados a Explotación con el fin de que éste:

    1. Copie el programa fuente en la Librería de Fuentes de Explotación, a la que nadie más tiene acceso
    2. Compile y monte ese programa, depositándolo en la Librería de Módulos de Explotación, a la que nadie más tiene acceso.
    3. Copie los programas fuente que les sean solicitados para modificarlos, arreglarlos, etc. en el lugar que se le indique. Cualquier cambio exigirá pasar nuevamente por el punto 1.

Como este sistema para auditar y dar el alta a una nueva Aplicación es bastante ardua y compleja, hoy (algunas empresas lo usarán, otras no) se utiliza un sistema llamado U.A.T (User Acceptance Test). Este consiste en que el futuro usuario de esta Aplicación use la Aplicación como si la estuviera usando en Producción para que detecte o se denoten por sí solos los errores de la misma. Estos defectos que se encuentran se van

corrigiendo a medida que se va haciendo el U.A.T. Una vez que se consigue el U.A.T., el usuario tiene que dar el Significado. Todo este testeo, auditoría lo tiene que controlar, tiene que evaluar que el testeo sea correcto, que exista un plan de testeo, que esté involucrado tanto el cliente como el desarrollador y que estos defectos se corrijan.

III.2.11.- AUDITORÍA INFORMÁTICA DE SISTEMAS.

Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las Comunicaciones, Líneas y Redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas.

Sistemas Operativos:

Engloba los Subsistemas de Teleproceso, Entrada/Salida, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas. Deben revisarse los parámetros variables de las Librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el constructor.

Software Básico:

Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al Software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agreda ni condiciona al Sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costes, por si hubiera alternativas más económicas.

Optimización de los Sistemas y Subsistemas:

Tunning: Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del Sistema en su conjunto. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal de Técnica de Sistemas.

Técnica de Sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de tunning pre programado o específico. El auditor verificará que las acciones de optimización fueron efectivas y no comprometieron la Operatividad de los Sistemas ni el plan crítico de producción diaria de Explotación.

Administración de Base de Datos:

El diseño de la Base de Datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general desarrollada en el ámbito de Técnica de Sistemas, y de acuerdo con las áreas de Desarrollo y usuarios de la empresa. Al conocer el diseño y arquitectura de éstas por parte de Sistemas, se les encomienda también su administración. Los auditores de Sistemas han observado algunas disfunciones derivadas de la relativamente escasa experiencia que Técnica de Sistemas tiene sobre la problemática general de los usuarios de Bases de Datos.

La administración tendría que estar a cargo de Explotación. El auditor de Base de Datos debería asegurarse que Explotación conoce suficientemente las que son accedidas por los Procedimientos que ella ejecuta. Analizará los Sistemas de salvaguarda existentes, que competen igualmente a Explotación. Revisará finalmente la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

Investigación y Desarrollo:

Como empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando Aplicaciones y utilidades que, concebidas

inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las Compañías del ramo. La auditoría informática deberá cuidar de que la actividad de Investigación y Desarrollo no interfiera ni dificulte las tareas fundamentales internas.

La propia existencia de aplicativos para la obtención de estadísticas desarrollados por los técnicos de Sistemas de la empresa auditada, y su calidad, proporcionan al auditor experto una visión bastante exacta de la eficiencia y estado de desarrollo de los Sistemas.

III.2.12.- AUDITORÍA INFORMÁTICA DE COMUNICACIONES Y REDES.

Para el informático y para el auditor informático, el entramado conceptual que constituyen las Redes Nodales, Líneas, Concentradores, Multiplexores, Redes Locales, etc. no son sino el soporte físico-lógico del Tiempo Real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en Comunicaciones y en Redes Locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de Redes Locales, diseñadas y cableadas con recursos propios).

El auditor de Comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la Red de Comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre la cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la Inoperatividad Informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La

contratación e instalación de líneas va asociada a la instalación de los Puestos de Trabajo correspondientes (Pantallas, Servidores de Redes Locales, Computadoras con tarjetas de Comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y a ser posible, dependientes de una sola organización.

III.2.13.- AUDITORÍA DE LA SEGURIDAD INFORMÁTICA.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.
La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial.

Ejemplo: Existe una Aplicación de Seguridad que se llama SEUS, para Unix, que lo que hace es auditar el nivel de Seguridad en todos los servidores, como ser: accesos a archivos, accesos a directorios, que usuario lo hizo, si tenía o no tenía permiso, si no tenía permiso porque falló, entrada de usuarios a cada uno de los servidores, fecha y hora, accesos con password equivocada, cambios de password, etc. La Aplicación lo puede graficar, tirar en números, puede hacer reportes, etc.

La seguridad informática se la puede dividir como Área General y como Área Especifica (seguridad de Explotación, seguridad de las Aplicaciones, etc.). Así, se podrán efectuar auditorías de la Seguridad Global de una Instalación Informática –Seguridad General- y auditorías de la Seguridad de un área informática determinada – Seguridad Especifica -.
Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática a nivel físico. Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptográficos.

El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes(incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

La decisión de abordar una Auditoría Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se elaboran “matrices de riesgo”, en donde se consideran los factores de las “Amenazas” a las que está sometida una instalación y los “Impactos” que aquellas puedan causar cuando se presentan. Las matrices de riesgo se representan en cuadros de doble entrada <<Amenaza-Impacto>>, en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

Ejemplo:

Impacto	Amenaza				
	1 Error	2 Incendio	3 Sabotaje	------	1: Improbable 2: Probable 3: Certeza - Despreciable
Destrucción de Hardware	-	1	1		
Borrado de Información	3	1	1		

El cuadro muestra que si por error codificamos un parámetro que ordene el borrado de un fichero, éste se borrará con certeza.

III.2.14.- P LAN DE C ONTINGENCIA.

Pese a todas las medidas de seguridad puede ocurrir un desastre. De hecho los expertos en seguridad afirman "sutilmente" que hay que definir un plan de recuperación de desastres "para cuando falle el sistema", no "por si falla el sistema". [9]

Por tanto, es necesario que el Plan de Contingencias que incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

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

Un **Plan de Contingencia de Seguridad Informática** consiste los pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del sistema, aunque, y por lo general, constan de reemplazos de dichos sistemas.

---

http://www.rediris.es/cert

Se entiende por Recuperación, “tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo, habiendo reemplazado o recuperado el máximo posible de los recursos e información”.

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

III.2.15.- EQUIPOS DE RESPUESTA A INCIDENTES.

Es aconsejable formar un equipo de respuesta a incidentes. Este equipo debe estar implicado en los trabajos proactivos del profesional de la seguridad. Entre éstos se incluyen:

- El desarrollo de instrucciones para controlar incidentes.
- La identificación de las herramientas de software para responder a incidentes y eventos.
- La investigación y desarrollo de otras herramientas de Seguridad Informática.
- La realización de actividades formativas y de motivación.
- La realización de investigaciones acerca de virus.
- La ejecución de estudios relativos a ataques al sistema.

Una vez que el Administrador de seguridad y el equipo de respuesta a incidentes han realizado estas funciones proactivas, el Administrador debe delegar la responsabilidad del control de incidentes al equipo de respuesta. Esto no significa que el Administrador no deba seguir implicado o formar parte del equipo, sino que no tenga que estar siempre disponible, necesariamente, y que el equipo debe ser capaz de controlar los incidentes por sí mismo.

El equipo será el responsable de responder a incidentes como virus, gusanos o cualquier otro código dañino, invasión, engaños, y ataques del personal interno. El equipo también debe participar en el análisis de cualquier evento inusual que pueda estar implicado en la seguridad de los equipos o de la red.

III.2.16.- B ACKUPS.

Un **backups** en informática es un archivo digital, un conjunto de archivos o la totalidad de los datos considerados lo suficientemente importantes para ser conservados.

El Backups de archivos permite tener disponible e íntegra la información para cuando sucedan los accidentes. Sin un backups, simplemente, es imposible volver la información al estado anterior al desastre.

Como siempre, será necesario realizar un análisis Costo/Beneficio para determinar qué información será almacenada, los espacios de almacenamiento destinados a tal fin, la forma de realización, las estaciones de trabajo que cubrirá el backups, etc.

Para una correcta realización y seguridad de backups se deberán tener en cuenta estos puntos:

1. Se debe de contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.
2. Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura/escritura, tipo de backup a realizar, etc.
3. El almacenamiento de los Backups debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.

4. Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenado, etc.

5. Se debe de contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.

6. Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por ejemplo, la información se debe encriptar antes de respaldarse.

7. Mantener equipos de hardware, de características similares a los utilizados para el proceso normal, en condiciones para comenzar a procesar en caso de desastres físicos. Puede optarse por:

- **Modalidad Externa:** otra organización tiene los equipos similares que brindan la seguridad de poder procesar la información, al ocurrir una contingencia, mientras se busca una solución definitiva al siniestro producido.
- **Modalidad Interna:** se tiene más de un local, en donde uno es espejo del otro en cuanto a equipamiento, características técnicas y capacidades físicas. Ambos son susceptibles de ser usados como equipos de emergencia.

Se debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios.

III.2.17.- PRUEBAS.

El último elemento de las estrategias de seguridad, las pruebas y el estudio de sus resultados, se lleva a cabo después de que se han puesto en marcha las estrategias reactiva y proactiva. La realización de ataques simulados en sistemas de pruebas o en laboratorios permiten evaluar los lugares en los que hay puntos vulnerables y ajustar las directivas y los controles de seguridad en consecuencia.

Estas pruebas no se deben llevar a cabo en los sistemas de producción real, ya que el resultado puede ser desastroso. La carencia de laboratorios y equipos de pruebas a causa de restricciones presupuestarias puede imposibilitar la realización de ataques simulados. Para asegurar los fondos necesarios para las pruebas, es importante que los directivos sean conscientes de los riesgos y consecuencias de los ataques, así como de las medidas de seguridad que se pueden adoptar para proteger al sistema, incluidos los procedimientos de las pruebas. Si es posible, se deben probar físicamente y documentar todos los casos de ataque para determinar las mejores directivas y controles de seguridad posibles que se van a implementar.

Determinados ataques, por ejemplo desastres naturales como inundaciones y rayos, no se pueden probar, aunque una simulación servirá de gran ayuda. Por ejemplo, se puede simular un incendio en la sala de servidores en el que todos los servidores hayan resultado dañados y hayan quedado inutilizables. Este caso puede ser útil para probar la respuesta de los Administradores y del personal de seguridad, y para determinar el tiempo que se tardará en volver a poner la organización en funcionamiento.

La realización de pruebas y de ajustes en las directivas y controles de seguridad en función de los resultados de las pruebas es un proceso iterativo de aprendizaje. Nunca termina, ya que debe evaluarse y revisarse de forma periódica para poder implementar mejoras.

III.2.18.- LA POLÍTICA.

Tiene la intención de ofrecer un acercamiento a una metodología sistemática en la importante tarea de administrar la Seguridad Informática.

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan ha llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de las empresas.

En este sentido, la política de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Definición de Políticas de Seguridad Informática.

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

Elementos de una Política de Seguridad Informática.

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

Parámetros para Establecer Políticas de Seguridad.

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.
- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícita y concretamente el alcance de las políticas con el

propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

III.2.19.- NIVEL FÍSICO.

El primer factor considerado, y el más evidente debe ser asegurar el sustrato físico del objeto a proteger. Es preciso establecer un perímetro de seguridad a proteger, y esta protección debe adecuarse a la importancia de lo protegido.

La defensa contra agentes nocivos conlleva tanto medidas proactivas (limitar el acceso) como normativas de contingencia (que hacer en caso de incendio) o medidas de recuperación (realizar copias de seguridad). El grado de seguridad solicitado establecerá las necesidades: desde el evitar el café y el tabaco en las proximidades de equipos electrónicos, hasta el establecimiento de controles de acceso a la sala de equipos.

Lo más importante es recordar que quien tiene acceso físico a un equipo tiene control absoluto del mismo. Por ello sólo deberían accederlo aquellas personas que sea estrictamente necesario.

III.2.20.- AMENAZA NO INTENCIONADA (DESASTRE NATURAL).

El siguiente ejemplo ilustra una posible situación:

Una organización no cuenta con sistemas de detección y protección de incendios en la sala de servidores. El Administrador del sistema deja unos papeles sobre el aire acondicionado de la sala. Durante la noche el acondicionador se calienta y se inicia un incendio que arrasa con la sala de servidores y un par de despachos contiguos.

Directivas:

1. **Predecir Ataque/Riesgo:** Incendio
2. **Amenaza:** Desastre natural. Incendio
3. **Ataque:** No existe.
4. **Estrategia Proactiva:**
    a. Predecir posibles daños: pérdida de equipos e información.
    b. Determinar y minimizar vulnerabilidades: protección contra incendios.
    c. Evaluar planes de contingencia: backup de la información.
5. **Estrategia Reactiva:**
    a. Evaluar daños: perdida de hardware e información.
    b. Determinar su origen y repararlos: bloqueo del aire acondicionado.
    c. Documentar y aprender
    d. Implementar plan de contingencia: recuperar backups.
6. **Examinar resultados y eficacia de la directiva**: Ajustar la directiva con los nuevos conceptos incorporado.

CAPITULO IV

IV.1.- PROPUESTA DEL TRABAJO DIRIGIDO.

Se puede considerar que el presente tema tiene una importancia, porque hoy en día la información depositada en la base de datos de una entidad pública no es muy segura porque cualquier funcionario de una entidad pública puede Borrar , modificar o sustraer información depositadas en la base de datos registrados en una computadora como por Ejemplo: Borraron información de las computadoras prefecturales de Cochabamba, la cual fue denunciado por el secretario general David Herrera de dicha prefectura, publicado en el periódico el Diario en fecha 04/09//08 para verificar dicha denuncia ver Anexos, en la cual se puede observar que una información depositada en la base de datos de una computadora ya no son bien seguras ya que por cualquier funcionario de una entidad pública se puede borrar o modificar una información.

La principal cualidad de este trabajo de investigación es la exploración respecto al tema de la seguridad informática, para así coadyuvar y proponer la uniformidad, regulación de la seguridad informática, que es necesaria para el resguardo de nuestros datos, será herramienta de gran beneficio para los responsables del manejo de la base de datos de la entidad pública, ejemplo como el Gobierno Autónomo Municipal de La Paz que no es muy seguro, el manejo de la información de los ciudadanos que manejan los funcionarios de la entidad pública.

Una de las principales falencias es la obtención de la información en la entidad pública ya que se niega al acceso de la misma, falta de conocimiento, respecto al tema por parte de nuestras autoridades, lo cual lo único que provoca es el retraso frente a estas necesidades.

Propuesta:

Mi propuesta es que se pueda crear una normativa jurídica especifica que regule principalmente la seguridad informática, mediante esta normativa legal para que se pueda garantizar la seguridad de nuestra información depositada en la base de datos de una entidad pública, ya que es necesario el resguardo de una información depositado en la base de datos de una entidad pública y por ende es importante el resguardo de nuestros datos que son muy importantes para la ciudadanía en general ya que se ocasiona un daño y perjuicio al titular de una información o a terceras personas y por ende deberían ser sancionados, algunos malos los funcionarios públicos de cualquier entidad pública ya sea por alterar o modificar una información que es muy valiosa para el desarrollo de nuestro país boliviano.

IV.2.- DIMENSIÓN Y ALCANCE DE LA PROPUESTA.

Se han analizado las causas y consecuencias de la inseguridad informática como problema de la investigación. En el presente trabajo se propone crear una normativa que regule la seguridad informática, ya que nuestra legislación en la materia de derecho informático referida al tema de seguridad informática se encuentra relegada, de esta manera se identifica la inexistencia de una normativa, en caso de que nuestra legislación cuente con alguna normativa conocer si se aplica la normativa general y uniforme que regule la seguridad de los datos que se encuentran depositado en la base de datos de la entidad pública ejemplo el Gobierno Autónomo Municipal de La Paz, generando un alto nivel de riesgo que la información, por diversos factores sean perdidas, modificadas, sustraídas, siendo dicha información de gran importancia para los ciudadanos.

IV.3.- CONCLUSIONES.

A manera de concluir el presente trabajo es necesario la protección de nuestros datos de manera legal, creando una normativa que regule la seguridad informática.

-No existe normativa específica que regule el tema de la seguridad informática en la base de datos de la Entidad Pública.

-La información depositada en las base de datos de las Entidad Publica se encuentra en un alto nivel de riesgo.

-La implementación de la normativa propuesta, en la Entidad Publica coadyuvara preventivamente en la temática de la seguridad informática otorgando a los encargados de las áreas de sistemas herramientas.

IV.4.- RECOMENDACIONES.

La socialización, discusión, del presente trabajo investigativo enriquecerá el desarrollo de la seguridad informática en las entidades públicas, ya que se debería crear una norma jurídica que regule la seguridad informática, que es un dato muy importante para el desarrollo de nuestro país.

Hoy en día la ciudadanía debería tener cuidado en depositar una información en cualquier entidad pública y verificar la información depositada constantemente, para que no sean modificados o sustraídos por cualquier persona.

BIBLIOGRAFÍA

- La nueva Constitución Política del Estado Plurinacional.
- Ley 2298 de Ejecución Penal y Supervisión.
- O.I.T.: Seguridad Social: Un nuevo consenso. Capítulo IV igualdad de género, informe de la comisión de la Seguridad Social, Conferencia Internacional del Trabajo, 89ava reunión. 2001.
- Reglamento de INASES.(Régimen de Corto Plazo)
- NEREN Miguel, "La técnica de recolección de información mediante los grupos focales". Biblioteca Virtual en Población. Centroamericano de Población. Revista Electrónica Nº. 7, En: http://huitoto.udea.edu.co/~ceo/
- Libro Introducción al estudio de la seguridad social, autor Dr. Iván Campero Villalba y Serapio Espada Lazcano, 5ta Edición, 2007.
- Apuntes de Seguridad social Dra. Nancy Tufiño.
- Apuntes de lecciones de derecho informático del Dr. Cesar Borgua Rodríguez.
- Osorio, Manuel "Diccionario de Ciencias Jurídicas, Políticas y Sociales" Editorial Heliasta 2204
- Cabanellas Guillermo, "Diccionario Enciclopédico de Derecho Usual", Editorial Heliasta S.R.L. 28ªEdiccion Buenos Aires Argentina.

- www.icalp.org.bo/
- http:/www. monografía. Com.htm.
- http//www.rediris.es/cert.
- http://www.cybsec. Com.
- http://www.agpd.es/ipload/Canal Documentación/ Estatal Ley 2015.
- Agencia Española de Protección de Datos Legislación Estatal

  https://www.agpd.es/index.php.seccion - 77
- Hispasec Sistemas. Servicios de Conformidad.

  http://www. hispasec. Com/ corporate.

ANEXOS

OPINION PERSONAL.

En la última década de estos años en nuestro país a estado viviendo una profunda transformación del estado en lo político, jurídico, económico y social, lo cual trajo para nuestra realidad la vivencia de muchas manifestaciones de la sociedad por la lucha de sus objetivos y materialización de los mismos, iniciando su lucha en octubre de dos mil tres, con la guerra del gas.

Hasta hace poco el 9 de septiembre de 2008 con la pretensión del golpe cívico prefectural, trayendo en los dos eventos como consecuencia la toma de entidades públicas, saqueo, robo de los equipos, la quema de la documentación y la información que se encontraba en ellas, un breve recuento de lo ocurrido en los años pasados, siendo en este contexto encausándonos en lo anterior lo que nos interesa en lo pasado y es la causal del tema de monografía es la perdida de la información en todos estos hechos, que paso con la información perdida, sabemos que existen medios de reposición de la información pero esto va mas allá es de tener la prevención y la seguridad de que nuestros datos que está depositada en las entidades y que las mismas estén más que preparados para este tipo de contingencias con normas que regulen de manera general a todas las entidades públicas.