41
24.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES.
"CAMPUS ARAGÓN"

"LA FUNCIÓN DE LA SEGURIDAD INFORMÁTICA DENTRO DE LAS ORGANIZACIONES"

T E S I S

Que para obtener el titulo de:

INGENIERO EN COMPUTACIÓN

P r e s e n t a:

ARIEL MOLINA FLORES

ASESOR: ING. BLANCA ESTELA CRUZ LUEVANO

SAN JUAN DE ARAGÓN 1997

A MIS PADRES:
Por darme la vida, un hogar, una familia y todo su apoyo para la realización de mis metas; por ser el ejemplo integro para mi formación; por ser maestros y guías en mi vida.

A MI ESPOSA GABY:
Por darme su amor y comprensión en todo momento; por todos los momentos felices pasados y aquellos que vendrán; por ser mi compañera y amor de toda la vida.

A MI HIJO CÉSAR:
Quien inicia una vida llena de satisfacciones, alegrias, triunfos pero también de derrotas y momentos amargos; a él para que esto le sirva como ejemplo de una de sus metas a lograr.

A XOCHITL, MEMO, MEMÍN E IVÁN:
A ellos por ser parte de mi motivación diaria para seguir adelante.

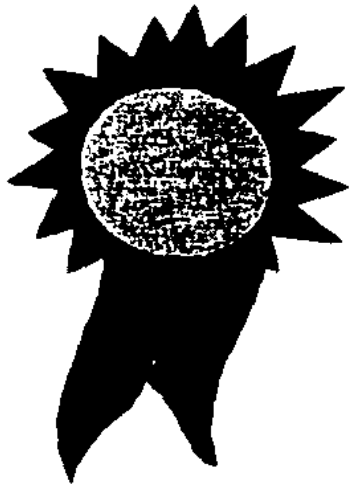
A MIS ABUELOS ROMAN Y ESTHER:
Por participar en mi formación como ser humano y como profesional; por sus valiosos consejos y por estar siempre al pendiente de todos en la familia.

A MIS PROFESORES:
Por compartir sus conocimientos y proporcionarme los consejos necesarios para mi desarrollo profesional.

A MIS AMIGOS JAVIER, GUILLERMO Y "LOS INFANTILES"
Por su amistad desinteresada y sin fronteras, por todos esos momentos gratos en los que hemos participado.

A MIS COMPAÑEROS DE UNIVERSIDAD:
Por los momentos difíciles y gratos que compartimos.

AL SEÑOR TODOPODEROSO
Por darme la oportunidad de vivir, sufrir, llorar y reir.



LA FUNCIÓN DE LA SEGURIDAD INFORMÁTICA DENTRO DE LAS ORGANIZACIONES

INDICE

CAPITULO I

INTRODUCCIÓN

De entre los escombros que ha dejado la crisis del "industrialismo", han surgido nuevos sectores productivos, tanto que las estructuras económicas viven un sorprendente proceso de mutaciones. Hasta hace poco tiempo se creyó que la riqueza de las economías se basaba en la producción y comercialización de productos tangibles, era impensable suponer que el desarrollo se orientara en otra dirección; sin embargo, y aunque *"todo empezó por proteger aspectos tangibles, las cosas han evolucionado hacia tecnologías más sofisticadas de protección de intangibles, como es la información"*.

Ahora la informática juega un papel cada vez más importante en aplicaciones que se llaman estrategias, las aplicaciones que le dan la razón de ser a las organizaciones. Antes teníamos aplicaciones para contabilidad, nóminas, inventarios y demás; ahora, ya la informática se utiliza para dar servicios a los clientes, incluso para apoyar los servicios que dan razón de ser a organizaciones como los bancos.

En este contexto la información adquiere una importancia decisiva; adquiere "un valor al igual que puede tener cualquier otro activo dentro de las organizaciones", sin embargo, es difícil darle valor monetario a una pieza de información, pero se considera que en un momento adecuado, una pieza de información puede ser la diferencia entre un buen o un mal negocio, entre el éxito y el fracaso.

Es importante advertir, para ubicar en sus justas dimensiones la importancia del tema, que analistas y hasta empresarios aseguran que el mundo se encuentra en la etapa de la "revolución de la información", la cual es fomentada en gran medida por el desarrollo y la penetración de la industria de la computación y las comunicaciones en las plantas de producción, los movimientos económicos y en casi todos los mercados. Esto le ha dado un fuerte impulso a las actividades relacionadas con la informática y los servicios que surgen alrededor de la misma.

México mismo, pese a la crisis y como efecto directo de la apertura comercial, ha sido alterado de un modo impresionante en el campo económico: el mercado nacional de la informática logró una impresionante expansión del 300% en sólo años, según datos oficiales de 1989 a 1994 pasó de 971 millones de dólares a 4,067 millones de dólares.

Lo anterior nos sirve para ubicar la importancia del valor de la información que, sin embargo, a estas alturas "todavía no existe un criterio generalizado para asignarle un valor". Todo mundo reconoce que tiene un valor estratégico y de muy importante peso económico. Por esta razón "hay que proteger la información, ya que puede estar sujeta a riesgos. Esta protección va más allá de proteger los medios informáticos en los cuales se encuentra, hay que proteger los flujos de información, hay que proteger el que no exista acceso no autorizado a la información y, sobre todo, también hay que contar con planes de contingencia para aquellos casos en que los servicios informáticos dejen de operar por cualquier razón".

¿Porqué proteger la información?

La información es un bien al que se le asocia un valor y que comparte, con otros bienes, el estar sujeta al riesgo. En la actualidad el valor de la información no sólo está asociado al impacto económico de las decisiones que se toman con base en ella y al costo de obtenerla y mantenerla sino a su autenticidad en lo que esa información representa.

Tal es el caso, por ejemplo, de los sistemas bancarios y de casas de bolsa en los que, incidentemente, el valor monetario de la información manejada por ellos representa varios ordenes de magnitud en monto de la inversión conjunta en equipo de cómputo, de telecomunicaciones y en desarrollo de sistemas (telemática).

Es por esto que la preocupación por proteger esa información ha recibido considerable atención en los últimos tiempos, sin embargo, ni el valor de la información ni la necesidad de seguridad son asuntos nuevos.

El presente trabajo está enfocado al conocimiento general de los elementos, piezas y controles de seguridad que se deben contemplar dentro de las organizaciones en donde sus flujos y procesos de datos estén estrechamente relacionados con tecnologías de información, es decir, equipos de cómputo, infraestructura de telecomunicaciones y metodología para el desarrollo de sistemas. Está organizado de la manera siguiente:

CAPITULO II.- ANTECEDENTES.- En este capitulo se presenta una breve historia de la seguridad en la información y se describe a grandes rasgos el camino que se ha recorrido hasta conocer el concepto de Seguridad Informática.

CAPITULO III.- CONCEPTOS GENERALES: El objetivo de este capitulo es el estandarizar los conceptos, definiciones y enfoques que a lo largo este trabajo se manejarán, es decir, para "hablar el mismo idioma".

CAPITULO IV.- ESTRUCTURA DE SEGURIDAD.- Se proponen los modelos de cobertura de la función de Seguridad Informática en los diferentes ambientes relacionados con el procesamiento de la información.

CAPITULO V.- CONTROLES BÁSICOS DE SEGURIDAD: En este capitulo se proporciona una guía genérica de los principios o elementos de inspección que deberán tomar en cuenta las organizaciones en sus procesos automatizados y en el manejo de información sensitiva. La implantación de estos controles estará en función de la tecnología y cada uno de ellos están susceptibles de ser complementados y reforzados para su mejora.

CAPITULO VI.- ANÁLISIS DE RIESGOS: El objetivo en este capitulo es proporcionar un panorama global de como se deben evaluar los niveles de seguridad en la información dentro de una organización por medio de metodologías cualitativas o cuantitativas y que pueden ser sustituidas con la adquisición de software especializado para estos fines.

CAPITULO II

ANTECEDENTES

Aún antes de la revolución industrial, la información ha sido un bien valioso. Desde que hay investigación sobre maquinaria, armas secretas, fórmulas químicas, secretos industriales y estrategias corporativas de mercadeo, aún en esos tiempos, la gente reconocía que cualquiera que controlara cierta información tenía un monopolio útil y por tanto estaba en posición de poder (ventaja competitiva) sobre los que no tenían esa información.

El advenimiento de las computadoras y la telecomunicación no ha introducido nuevos aspectos sino ha transformado la naturaleza de los ya existentes. Históricamente, el papel moneda y los metales preciosos estuvieron resguardados en cajas fuertes y bóvedas de acero y concreto; hoy la mayor parte del dinero se almacena en forma electrónica dentro de sistemas de cómputo, que son las nuevas cajas fuertes y bóvedas de seguridad. Por tanto, el enfoque actual es hacer los sistemas informáticos más seguros para proteger, por ejemplo, el dinero electrónico y la información sensible relativa a las organizaciones y a los individuos.

En un principio, al iniciarse la comercialización de las computadoras, el acceso solo era permitido a un reducido número de especialistas en el área. Sin embargo, en la actualidad al aumentar de manera extraordinaria el número de sistemas de cómputo, la interacción directa con las computadoras y sus datos se volvió algo rutinario para un gran número de usuarios, hasta para los casuales. Este ambiente abierto, consecuentemente, ha aumentado la dificultad para mantener la seguridad. Por otro lado, el hecho de que cada vez mas personas cuentan con los conocimientos suficientes para programar, penetrar y manipular sistemas de cómputo y que además la información manejada en estos sistemas pueda tener un valor suficiente como para tentar a algunas personas a intentar tener acceso a ella, ha originado una mayor preocupación, tanto de proveedores como de usuarios, para lograr un nivel satisfactorio de seguridad en los sistemas de cómputo. Estos factores han originado que se establezcan normas, políticas, estándares, procedimientos y controles en los sistemas de cómputo.

Actualmente cientos de miles de computadoras, con gran variedad de características, se encuentran instaladas en oficinas, escuelas, fabricas, hospitales, bancos, tiendas y hogares debido a la gran importancia que han adquirido los sistemas de cómputo en la sociedad moderna, se ha creado la necesidad de garantizar la

seguridad de la información, programas y del equipo necesario para su procesamiento. Ya que el uso cada vez mas extendido de los sistemas de computo incrementa los riesgos de sufrir abusos en el manejo de las computadoras o bien desastres a causa de robo, fraude, sabotaje o interrupción en las actividades de cómputo, la función de Seguridad Informática deberá encargarse de la protección de los datos almacenados contra el manejo accidental o mal intencionado de estos; así como también, de la protección física del equipo y aplicaciones de cómputo, con el fin de disminuir el riesgo de ser dañados o destruidos.

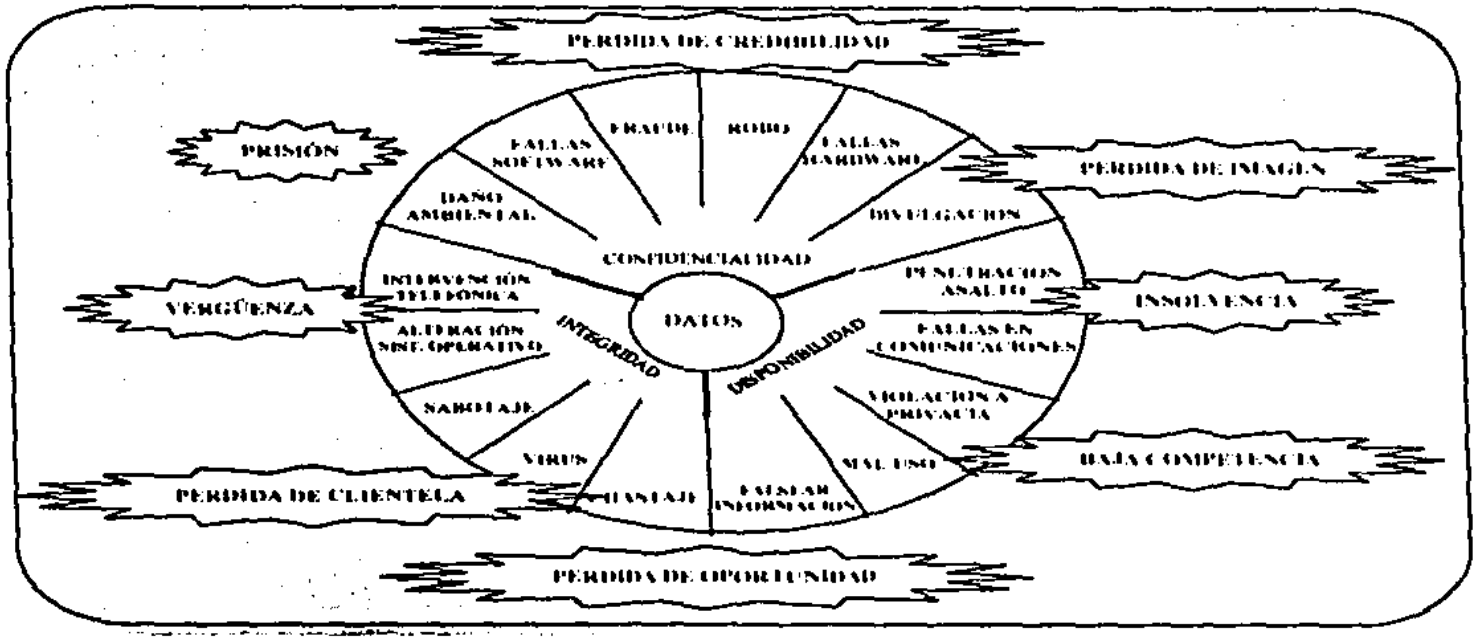
Durante los últimos años los fabricantes de productos informáticos, especialistas en el tema, usuarios y publico en general, han reflexionado y tomado conciencia de la importancia que debe de darse a la seguridad informática, que anteriormente había sido relegada a un segundo término. En México este tipo de seguridad es una especialidad nueva que empieza a darse a conocer y que tiene un futuro muy prometedor. Algunas pruebas de la gran preocupación existente por mejorar la seguridad de los sistemas de cómputo lo

son el incremento en el número de artículos, reportajes y editoriales que hacen alusión al tema, publicados no solo en revistas y periódicos especializados, sino hasta en los periódicos de circulación con mercado hacia toda la sociedad. Otro indicador es el gran número de productos, tanto de hardware como de software, especializados en seguridad informática que han proliferado en el mercado internacional y que ha incrementado su introducción al mercado nacional. Un indicador más de la preocupación en estos rubros, es el revuelo que causo en todos los medios de la sociedad la activación del virus informático llamado "Miguel Ángel", durante el mes de marzo de 1992.

Con base en situaciones como las antes expuestas es que surge la inquietud de realizar un estudio que trate el tema de la Función de Seguridad Informática dentro del contexto de nuestra realidad nacional, en el cual se proponen esquemas de seguridad informática aplicables a las organizaciones en México.

Con los conceptos vertidos en el presente trabajo, los niveles directivos responsables de la organización, deberán tomar la iniciativa para definir la directrices y establecer la Función de Seguridad Informática, la cual a su vez revisará, definirá, actualizará y difundirá los modelos y estrategias de seguridad en la información.

MISIÓN DE LA FUNCIÓN

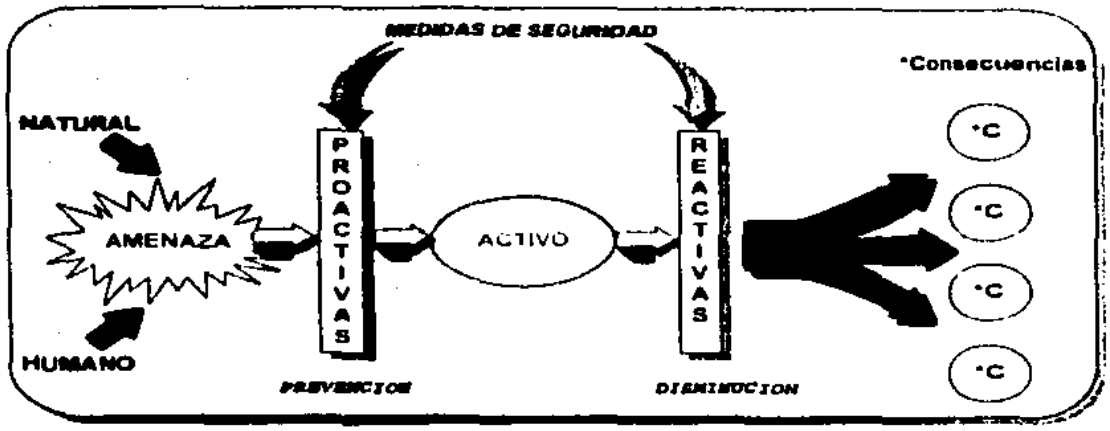


La figura anterior representa los riesgos y efectos a los cuales la organización esta expuesta de manera directa o indirecta ante la pérdida de seguridad en la información.

Cuando nos referimos a la misión de una empresa, departamento, función, etc., hablamos de la filosofía o razón de ser de la misma; la misión de la función de Seguridad Informática es la de preservar la Integridad, Confidencialidad y Disponibilidad de la información contra la Divulgación, Modificación, Destrucción y Mal Uso por medio de la Prevención, Detección y Recuperación para una reducción de pérdidas o riesgos de pérdidas.

En otras palabras, la misión es mantener un alto nivel de seguridad en los atributos de la información aplicando tecnología y desarrollando e instrumentando estrategias y acciones tendientes a administrar los riesgos (asumiendo, transfiriendo, minimizando o eliminando) derivados del diseño, operación y administración de los principales procesos automatizados y manuales de la Organización.

OBJETIVO



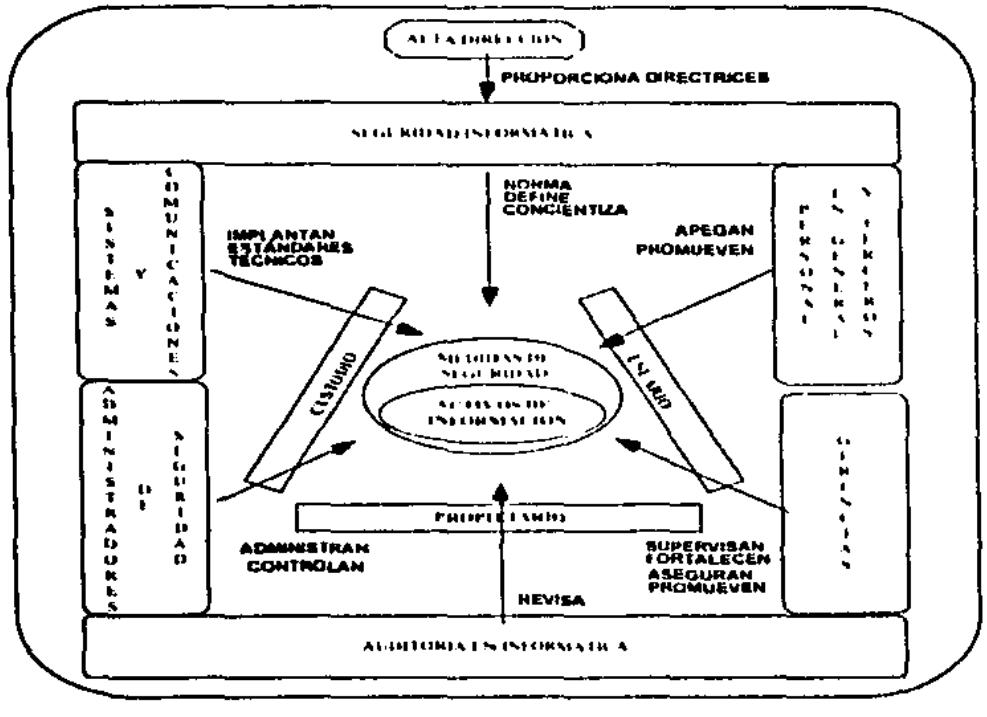
El objetivo de la Función de Seguridad Informática es el establecimiento de programas proactivos que involucren estrategias y arquitecturas tecnológicas aplicables en toda la Organización para salvaguardar los activos en materia de información.

Un ambiente positivo de programas de seguridad proactivas será necesario para el uso, a nivel staff, de seguridad en la información en cuanto a la definición de roles, ayuda a los departamentos usuarios para apoyar sus necesidades de seguridad y definición de modelos y estrategias para protección de la información.

Los recursos de información incluyen la información por si misma en todos sus medios, el hardware y software, equipos de comunicaciones, y la construcción de elementos de infraestructura relacionados (por ejemplo, electricidad y sobrecalentamiento, ventilación y aire acondicionado). *En todos los ambientes de procesamiento de información, el recurso más importante es la gente.*

Bajo este contexto, es importante notar que los programas de protección a la información deberán ser dirigidos hacia la administración de actividades técnicas y de la misma gente. Los componentes administrativos de los programas de protección, son generalmente más importantes y más difíciles de implementar que los elementos técnicos. Los programas no deben ser desarrollados únicamente desde el punto de vista técnico, la completa participación de la Alta Dirección es el factor crítico de éxito ya que sin su sensibilización, apoyo y directrices, difícilmente se lograrán los objetivos de la Función de Seguridad Informática.

ALCANCE



La función y los conceptos de seguridad informática deberán ser de carácter general para toda la organización y corresponderá a todo el personal, promover un ambiente en el cual el manejo de la información sea seguro.

Se proponen los responsables de manera genérica según su competencia:

Alta Dirección

Departamento de Seguridad Informática

Áreas de Sistemas y Telecomunicaciones

Departamento de Administradores de Seguridad

Departamento de Auditoría Informática

Gerencias

Personal en General.

RESPONSABILIDADES

Dirección administrativa.- Es la entidad cuyo propósito es establecer las directrices y autorizar las estrategias que permitan fortalecer en la Organización, las medidas de seguridad informática y cuyas funciones son:

- Establecer directrices sobre esta materia de seguridad informática.
- Autorizar estrategias, políticas y programas de acción en este aspecto.
- Revisar los resultados de los diferentes programas de acción implantados.
- Dar solución a los problemas de seguridad informática.

Departamento de Seguridad Informática.- Tiene a su cargo definición de políticas, normatividad, medidas de seguridad y dar apoyo en este aspecto a todas la áreas de la Organización, además:

- Define y establece estrategias, modelos y arquitectura en materia de seguridad de la información y continuidad de servicio en conjunto con las áreas correspondientes.
- Establece y mantiene las políticas y normas generales en materia de seguridad informática.
- Realiza evaluaciones y diagnósticos de riesgos para identificar vulnerabilidades y señalar acciones de solución.
- Investiga tecnología de vanguardia para la protección de la información en todos sus medios y formas en conjunto con las áreas involucradas.
- Propone, define y fija mecanismos y medidas para fortalecer la seguridad en la información.
- Certifica que las herramientas tecnológicas utilizadas y propuestas por las áreas de sistemas, responsables del diseño e implantación de medidas específicas, cuenten con los elementos mínimos necesarios de seguridad informática.
- Dar apoyo a los gerentes de las unidades organizacionales en materia de seguridad informática cuando así lo soliciten.
- Promueve en la Organización programas de concientización y capacitación en materia de seguridad informática.

Áreas de Sistemas y Telecomunicaciones.- Entidades relacionadas con el manejo, proceso y manipulación de la información utilizando tecnología para tales fines.

- Aseguran que se cumplan las normas, los procedimientos y estándares vigentes en seguridad informática que se encuentren dentro de su ámbito de responsabilidad.
- Instrumentan esquemas y herramientas de seguridad informática en la arquitectura conceptual de hardware, software y aplicaciones de comunicaciones, apegándose a las políticas y normas definidas por el Departamento de Seguridad Informática y satisfaciendo los requerimientos de los Responsables de la Información.

- Desarrollan e implementan software de infraestructura y estándares técnicos de seguridad informática conforme a los lineamientos establecidos por el Departamento de Seguridad Informática.
- Garantizan la correcta instalación y liberación de los esquemas y herramientas de seguridad informatica.

- Dan mantenimiento y soporte a esquemas y herramientas requeridas y sustentadas en las normas y políticas institucionales de seguridad informática.
- Investigan y evalúan herramientas tecnológicas de seguridad informática con apego a los requerimientos del Departamento de Seguridad Informática

Departamento de Administradores de Seguridad.- Tiene a su cargo la administración de usuarios en el acceso y sus facultades en las aplicaciones, plataformas tecnológicas, así como la administración de redes locales.

- Controlan la asignación de los accesos y otorgamiento de facultades a los usuarios y atributos en el medio ambiente aplicativo y técnico, si corresponde.
- Dan mantenimiento y actualizan los parámetros y catálogos utilizados por los esquemas de acceso y facultades.
- Como custodio del ambiente de seguridad, establecen y vigilan la continuidad, recuperación y actualización oportuna de los usuarios y recursos.
- Dan seguimiento a situaciones de excepción en actividades relacionadas a la seguridad, reportando éstas a sus niveles de Dirección y al Departamento de Seguridad Informática.
- Plantean y detectan problemas referentes a la seguridad de la información.

Departamento de Auditoría Informática.-

- Audita el cumplimiento y suficiencia de las políticas y normas de seguridad informática, informando sobre el apego a las mismas por parte de los involucrados.
- Revisa y evalúa los controles de seguridad y los esfuerzos en desarrollo para la implementación de los mismos.

Gerencias.- Los gerentes de las áreas, departamentos o unidades organizacionales para fines de la protección de la información, son los responsables de la misma, cumpliendo lo que a continuación se detalla:

- Introducir e involucrar los conceptos, medidas y mecanismos de seguridad informática dentro de su ámbito de responsabilidad y en la normatividad y procedimientos que realicen para apoyar su función.
- Vigilar y supervisar el cumplimiento de las políticas y normas de seguridad informática.
- Apoyar y dar información para la realización de diagnósticos de riesgos y minimización de los mismos.
- Atender y dar seguimiento a los riesgos detectados por el Departamento de Seguridad Informática y en su caso se asuma o acepte, deberá constar por escrito en un documento avalado con su firma.

- Realizar pruebas que certifiquen el esquema de seguridad bajo el cual trabajan sus sistemas automatizados.
- Promover la difusión de las medida y mecanismos de seguridad para consolidar la confianza con el personal, clientes y proveedores mediante la protección de loas activos propiedad de la Organización.

- En base a las instrucciones del Departamento de Seguridad Informática, mediante un estudio específico, tomar decisiones de seguridad relativas a la protección de los activos de información.
- Delegar responsabilidad operacional para la protección de los activos de información.
- Considerar en la evaluación de su personal el cumplimiento a las políticas de seguridad en la información, definidas en la normatividad vigente.
- Implantar y dar seguimiento a los programas de concientización de seguridad informática que se establezcan para garantizar el uso de las herramientas para tal fin.
- Detectar y plantear problemas sobre seguridad de información al Departamento de Seguridad Informática.

Personal en General.- Por una posición ética y profesional, todo el personal, independientemente de su función y jerarquía, debe impulsar y promover la seguridad en la institución en todas y cada una de sus actividades y acatar todas las disposiciones al respecto, aceptando las consecuencias laborales y legales por no cumplirlas; dentro de estas disposiciones destacan las siguientes:

- Conocer y acatar la normatividad aplicable en materia de seguridad informática.
- Ni divulgar ni modificar información confidencial sin autorización expresa de acuerdo con las facultades conferidas, no permitir a otra persona el acceso a la misma.
- Cooperar en la realización de Campañas de Concientización que en materia de seguridad informática se realicen en la Organización, proporcionando información que se le solicite y con actitud positiva.
- Emprender todas las medidas de seguridad informática aplicables a su función y que de manera enunciativa más no limitativa se enlistan:

  Utilizar con seguridad y responsabilidad sus claves de acceso.

  Respetar el acceso a los lugares de cómputo.

  Realizar eficientemente los respaldos de su información.

  Utilizar el software autorizado sin hacer copias ilegales.

  Utilizar el equipo sólo de acuerdo con las facultades asignadas.

  Apegarse a la normatividad establecida para manejar de manera segura la información en todos sus medios y formas.

- Dar seguimiento a las medidas y mecanismos de seguridad informática.
- Reportar irregularidades detectadas en las instalaciones de trabajo al supervisor de área o jefe inmediato y atender las indicaciones establecidas en la normatividad de seguridad informática.

- **Reconocer la propiedad de la Organización sobre todos los productos, aplicaciones e información desarrollada por los empleados.**
- **Aplicar el código de ética existente en la Organización.**

CAPITULO III

CONCEPTOS GENERALES

En este capitulo se definen los términos y conceptos que se manejarán en el transcurso de dicho trabajo con la finalidad de hacer de fácil acceso y entendimiento las expresiones "técnicas" utilizadas.

RIESGO.- Es la probabilidad que una amenaza particular se convierta en una vulnerabilidad para el sistema.

AMENAZA.- Se define como una ocurrencia potencial o un evento no deseado que puede producir daño tanto a un sistema como a la organización. En otras palabras, las amenazas son diferentes actos o eventos que la organización desea prevenir. Definitivamente se quiere prevenir amenazas como pérdida de datos, robo, desastres e interrupciones, errores y omisiones, divulgación no autorizada, acceso ilegal, etc., etc.

Es un evento o método que potencialmente puede comprometer la integridad, disponibilidad o confidencialidad en un sistema de procesamiento de información.

MUESTRAS DE ALGUNAS AMENAZAS

PÉRDIDA DE PRIVACIDAD.- Acceso no autorizado a información o datos confidenciales.

ERRORES Y OMISIONES.- Errores que ocurren durante la preparación, procesamiento o generación de información.

ACCESO ILEGAL AL SISTEMA.- Acceso no autorizado a bases de datos, redes, programas de cómputo, documentos sensitivos, etc.

FRAUDE O ROBO.- Robo de información o datos de la organización o sus activos como son: manuales o estrategias, haciendo uso de la red de la organización

PÉRDIDA O CORRUPCIÓN DE MENSAJES.- Mensajes equivocados o mal dirigidos, pérdida, no procesamiento o retraso de los mismos, que pudiera ocurrir de manera manual, durante proceso electrónico o por medio de la red.

DESASTRES O INTERRUPCIONES.- Desastres físicos incluyendo fuego, inundación, fallas eléctricas, tormentas, sismos, nevadas, etc.

COMPONENTES.- Es definido como una parte específica de un sistema; por ejemplo, cuando se ensambla algún mecanismo, los componentes de un sistema hacen el universo del mismo. Análogamente, los componentes de un automóvil, son las llantas, la dirección, el motor, la carrocería, etc. Los componentes de un sistema de cuentas por pagar deberá incluir chequeras, cargos y abonos, circuitos de comunicación, terminales, programas, y la gente que opera el sistema. En otras palabras, *los componentes pueden ser vistos como los elementos sobre los cuales se desea mantener control.*

MUESTRAS DE ALGUNOS COMPONENTES

REPORTES.- Reportes y archivos manuales, documentos, bitácoras, etc.

MICROCOMPUTADORAS Y TERMINALES.- Equipo conectado a un mainframe o red.

MAINFRAME O MINICOMPUTADORAS.- El centro de cómputo, discos y cintas, y otros periféricos físicos.

OPERADORES DE TERMINALES.- Operadores, empleados temporales, proveedores y todo tipo de personal que tenga acceso a las terminales de la organización.

CIRCUITOS DE COMUNICACIONES.- Circuitos de comunicación que conectan a la organización a WANs (Wide Area Networks) o LANs (Local Area Networks).

BASES DE DATOS.- Datos organizados en archivos o medios magnéticos, cintoteca y sites de respaldo.

PROGRAMAS.- Software y programas aplicativos para mainframes y microcomputadoras.

VULNERABILIDAD.- Es una debilidad en los procedimientos de seguridad, diseño de sistemas, implementación y controles internos que pueden reflejarse en la violación de las políticas de seguridad.

INFORMACIÓN SENSITIVA.- Es la información que deberá ser protegida debido a que su divulgación no autorizada, alteración, pérdida o destrucción puede causar un daño sustancial a la Organización.

ENCRIPCIÓN.- Es la transformación de datos por medio de técnicas criptográficas para producir texto indescifrable.

CONTROLES.- Acciones, técnicas, procedimientos o cualquier medida para la protección y reducción de grados de exposición de activos.

CONTROLES DE SEGURIDAD.- Es una política, método, práctica, dispositivo o un mecanismo programado para evitar o denegar, prevenir o detectar, mitigar, sancionar, transferir, recuperar o corregir pérdida de información además de incluir técnicas y métodos para asegurarse que únicamente los usuarios autorizados puedan accesar el sistema de cómputo y a todos sus recursos.

CONTROLES BÁSICOS.- Cada uno de los controles o medidas de seguridad que deben adoptarse como mínimo en aquella Organización que requiera proteger su información de caracter sensitivo.

POLÍTICA DE SEGURIDAD.- Es una serie de leyes, reglas y prácticas para regular como una organización debe administrar, proteger y distribuir información sensitiva.

Las políticas y normas se pueden definir como directrices de actuación aplicables en las situaciones que se presenten en el área de informática, para la toma de decisiones. Para diferenciar estos elementos hay que considerar los siguientes aspectos:

POLÍTICAS.- Criterios, principios y directrices las cuales son genéricas, flexibles, permiten la iniciativa, permiten el uso de criterio y permiten la interpretación.

<u>NORMAS.-</u> Reglas de conducta de carácter obligatorio, son específicas, rígidas o estrictas, existen sanciones por su no aplicación, evitan la iniciativa, no se puede aplicar el criterio, así como existe poca posibilidad de interpretación.

<u>NORMA DE SEGURIDAD INFORMÁTICA.-</u> Control básico de seguridad llevado a la categoría de regla de carácter obligatorio, que no indica de manera detallada la forma de llevarse a la práctica, y por lo tanto, es genérica para las plataformas tecnológicas a la que se debe aplicar.

<u>ESTÁNDARES.-</u> son unidades de medida que sirven como modelo o guía a cumplir para realizar las actividades tendientes al logro de objetivos. Los estándares en caso de la informática, pueden ser de tres tipos:

<u>De uniformidad</u>: son aquellos que tienen como propósito facilitar la compatibilidad, conectividad, transportabilidad y comparacion de datos. Así como en forma indirecta la actualización o mantenimiento y la introducción de personal.

<u>De rendimiento o productividad</u>: son los que permiten establecer el nivel de eficiencia y eficacia que deben tener las personas, equipos y procedimientos del área de informática.

<u>ESTÁNDARES DE SEGURIDAD.-</u> Control de seguridad que indica la forma específica de llevarse a la práctica para un ambiente o plataforma en particular. Si se requiere una serie de actividades para satisfacerla se le denomina procedimiento de seguridad informatica.

<u>PROCEDIMIENTOS.-</u> son el conjunto de pasos o actividades previamente establecidos que serán ejecutados en un orden específico para el logro de un objetivo.

<u>ESQUEMA DE SEGURIDAD INFORMÁTICA.-</u> Sistema de controles formado por normas, políticas, estándares, procedimientos y herramientas de seguridad informatica que interactuan para preservar los atributos de la información que protegen.

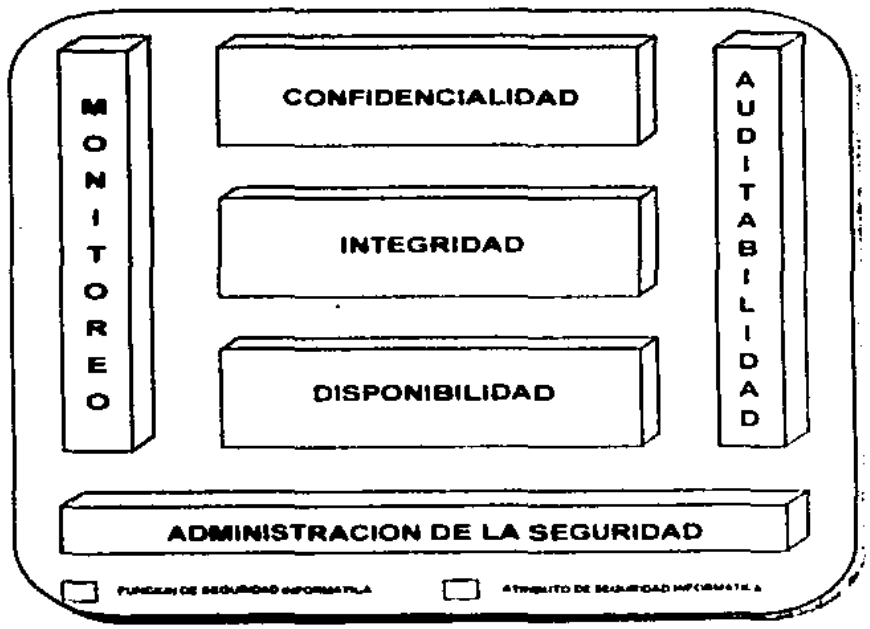
<u>HERRAMIENTAS DE SEGURIDAD INFORMÁTICA.-</u> Componente de hardware o software que sirve para efectuar una función (o parte de ella) de seguridad informática. Ejemplo de esto son el software antivirus, encriptores de señales en líneas telefónicas, sistemas para el control y administración de usuarios, etc.

ATRIBUTOS DE LA INFORMACIÓN

Hemos hablado en el transcurso de este trabajo en innumerables ocasiones de la información, pero, ¿qué es la información?. La información se define como el conocimiento que se tiene de algo, es la averiguación que se tiene de un hecho o una causa, en informática, es el contenido de los mensajes transmitidos por diferentes medios.

La información en términos generales, tiene un considerable número de características y cualidades como son la veracidad, la claridad de los mensajes, las fuentes de información, la oportunidad y vigencia, su importancia y relevancia, etc., etc.

Para fines del establecimiento de la función de Seguridad Informática se considerarán los siguientes atributos básicos que deberán ser preservados así como las funciones elementales que deberán ser implantadas y reconocidas para la salvaguarda de la información.



EL MODELO ANTERIOR ESQUEMATIZA LOS ATRIBUTOS Y FUNCIONES BÁSICAS DE SEGURIDAD QUE DEBERÁ PRESERVAR LA INFORMACIÓN

CONFIDENCIALIDAD

A) Es la característica que asegura el acceso a los recursos informáticos, aplicaciones y datos a aquellos entes autorizados de acuerdo con sus funciones y responsabilidades, protegiendo de esta forma la información contra consulta y divulgación no autorizada.

B) Característica que garantiza la privacía de información sensitiva.

ELEMENTOS A CONSIDERAR

- Clasificación de la información
  - Altamente restringida
  - Confidencial
  - Pública
- Control de acceso a la información y sus vistas
  - Identificación
  - Autentificación
  - Autorización
- Manejo de facultades de acuerdo con el perfil de la responsabilidad y la función
  - Altas
  - Bajas
  - Cambios
  - Consultas
- Manejo de identificadores de usuario y claves de acceso (Users ID & Passwords).
  - Asignación
  - Cambio
  - Bloqueo/desbloqueo
  - Cancelación
- Distribución de información
  - Electrónica
  - Medios removibles
  - Impresa
- Control de mecanismos de encripción y autentificación.
  - Transmisión
  - Almacenamiento

INTEGRIDAD

A) Es la característica que asegura que la información es genuina, completa y exacta, garantizando la protección de la información contra la modificación no autorizada y/o accidental.

B) Característica que garantiza que la información y programas son modificados solamente de manera específica y autorizada.

ELEMENTOS A CONSIDERAR

- Consistencia
  - Elementos propios del proceso
  - Interfases
  - Esquemas de estructura
  - Control de versiones
  - Estandarización de componentes
- Correspondencia
  - Entre resultados de la salida contra resultados esperados
  - Direccionamiento de transacciones entre aplicaciones
  - Ruteo de mensajes entre dispositivos
- Información completa en:
  - Elementos
  - Contenido
  - Procesamiento
- Validación
  - Procesos
  - Datos
  - Transacciones
  - Ruteo de mensajes
  - Cifras control
- Control de replicas en:
  - Aplicaciones
  - Software
  - Datos

DISPONIBILIDAD

A) Es la característica que asegura la continuidad y oportunidad en el otorgamiento de servicios automatizados de la Organización así como su la operación interna.

B) Propiedad que garantiza que los sistemas trabajen adecuadamente y que el servicio no sea negado a usuarios autorizados.

ELEMENTOS A CONSIDERAR

- Puntos de reinicio y recuperación
- Planes de contingencia
  - Definición de las funciones criticas del negocio
  - Procedimientos
  - Mecanismos de respaldo de software y bases de datos
  - Administración de recursos
- Auto-respaldo
  - Aplicaciones
  - Plataformas tecnológicas
  - Comunicaciones
- Funcionalidad de operación
  - Hardware
  - Software
  - Comunicaciones

AUDITABILIDAD

A) Es la capacidad funcional que permite rastrear y registrar los eventos ocurridos en materia de seguridad sobre dispositivos, aplicaciones, usuarios, oficinas, transacciones y mensajes.

ELEMENTOS

- Pistas de auditoría
  - Operación de procesos críticos

- Rastreo sobre los componentes de los procesos

- Registro de eventos
  - Cambios de los atributos o parámetros de seguridad
  - Afectación de la seguridad de los procesos

- Reporte de excepciones
  - Intentos de violaciones
  - Cambios de los atributos o parámetros de seguridad
  - Afectación de la seguridad de los procesos

- Revisión y seguimiento de bitácoras
  - Validación y apego a normas establecidas
  - Detección de desviaciones no atendidas para su corrección

Los siguientes elementos no son considerados como atributos de la información, son mejor dicho, funciones que deberán realizarse por la figura del Administrador de la Seguridad con apoyo del Departamento de Seguridad en Informática.

MONITOREO

A) Es la detección y registro en línea de eventos significativos de seguridad ocurridos fuera de los parámetros permitidos con el fin de facilitar su atención y solución inmediata.

FUNCIONES

1. Determinar los principales procesos, dispositivos, aplicaciones, plataformas tecnológicas y medios de comunicaciones a vigilar en cuanto a su comportamiento en seguridad.
2. Detectar y registrar de manera automática y en línea situaciones significativas de afectación a la seguridad.
3. Reportar y canalizar de manera inmediata la situación significativa de seguridad al área responsable correspondiente.
4. Atender y dar solución a las situaciones significativas de afectación a la seguridad generadas como consecuencia de eventos contingentes.
5. Actualizar periódicamente los parámetros de seguridad de acuerdo a las necesidades de protección vigentes.

ADMINISTRACIÓN DE LA SEGURIDAD

A) Se orienta a manejar y controlar los recursos y atributos de seguridad con el fin de asegurar la protección de la información, así como la administración de las herramientas de seguridad para cada plataforma tecnológica.

FUNCIONES

1. **Controlar altas, bajas y cambios de archivos de seguridad**
   - **Usuarios**
   - **Claves de acceso**
   - **Tablas de facultades**

2. **Generar indicadores estadísticos para actualizar y evaluar el comportamiento de los eventos y atributos de seguridad.**

3. **Parametrizar y asegurar la vigencia de los lineamientos de seguridad.**

4.- Garantizar la correcta instalación, liberación, mantenimiento y soporte de los esquemas y herramientas de seguridad.

5.- Dar seguimiento a situaciones de excepción, reportando éstas a sus niveles de dirección y a la Función de Seguridad Informática.

6.- Desarrollar e implantar estándares técnicos de seguridad de acuerdo a los lineamientos de la Función de Seguridad Informática.

7.- Concientización y difusión de la seguridad sobre activos informáticos al personal de su plataforma tecnológica.

CLASIFICACIÓN DE LA INFORMACIÓN.

¿Porque se necesita clasificar la información?

La información cada vez más ha sido desarrollada y utilizada para funciones críticas de la Alta Dirección. El crecimiento del número de computadoras y el incremento de demanda de datos por parte de la Alta Dirección ha contribuido a la proliferación de datos sensitivos y consecuentemente, a la necesidad de mantener un mejor control de acceso a esa información.

Esta dependencia de información también ha conducido a incrementar la demanda de información en tiempo real y accesos en línea a los datos. El Intercambio Electrónico de Datos (EDI) y la expansión de la globalización de redes de comunicaciones, reflejan un crecimiento en la dependencia de la conectividad de recursos. Así es como la conectividad a crecido de manera exponencial y por ende la vulnerabilidad en el control de acceso no autorizado a la información.

Reconociendo esos riesgos, la Alta Dirección deberá incrementar los niveles de protección a la información; el costo de los controles para proteger información sensitiva deberá ser dimensionado en base a los recursos de la empresa y a un plan de recuperación de desastres ante una contingencia. La Alta Dirección puede ser apoyada en el manejo y administración de la información en recursos y controles, a través de un buen esfuerzo para llevar a cabo un programa de clasificación de información el cual esté perfectamente documentado y aceptado.

La información como un activo de la Organización.

Toda la información mantenida por una corporación tiene valor tangible e intangible, como aquella que ha sido desarrollada dentro de la compañía o comprada. La compañía deberá decidir la restricción al acceso a dicha información si determina que el acceso no autorizado pudiera disminuir el valor de la información, proporcionar ventaja a la competencia o violar obligaciones legales debido a la divulgación; por ejemplo, análisis de mercado, proyecciones de ventas, e investigación y desarrollo de tecnología de vanguardia.

Niveles de Sensitividad.

Muchas organizaciones encuentran cuatro categorías para identificar y agrupar la información en base a su grado de sensitividad, estas categorías son listadas en orden ascendente de sensitividad:

- Información Pública
- Información Sensitiva
- Información Restringida
- Información Secreta.

INFORMACIÓN			
PÚBLICA	***SENSITIVA***	***RESTRINGIDA***	***SECRETA***
Típicamente alguna información de la organización es considerada apropiada para su divulgación al público en general a través de noticias, o documentos públicos. Por medio de esta información puede estar la clave del éxito de la organización o un proyecto.	Esta información deberá estar disponible únicamente para los empleados de la compañía más no para el público en general. Ejemplo de esto son los planes generales de un producto específico o una base de datos que la compañía ha invertido demasiados recursos para su desarrollo. La pérdida de esta información pudiera proporcionar ventaja a la competencia o desconcertar a la compañía si es revelado en una manera no apropiada.	Este tipo de información deberá ser limitado a un número limitado de personal definido por el propietario de los datos. Investigación y desarrollo de datos asociados con un plan estratégico, parámetros de seguridad de un software o claves de acceso para un equipo de computo, son ejemplos de información restringida. La entrega o descubrimiento de este tipo de información pueden resultar en una variedad de daños, desde pérdida de confidencialidad de un cliente hasta el sabotaje de planes estratégicos.	Este tipo de información solamente debe estar disponible para un muy limitado numero de usuarios. El acceso a este tipo de información deberá ser controlado utilizando bitácoras de firmas supervisadas, generalmente, por el propietario de la información.
EJEMPLOS HACIA QUIEN ESTA DIRIGIDA LA INFORMACIÓN			
• Clientes y Proveedores	• Empleados de la compañía	• Grupos de trabajo • Tareas especiales	• Miembros de Dirección • Vicepresidencia de mercado y área Staff inmediata.

Existen otras clasificaciones de información desde puntos de vista de sus atributos.

CLASIFICACIÓN POR DISPONIBILIDAD			
TIPO DE INFORMACIÓN	**CATEGORÍA**	**PÉRDIDA POTENCIAL**	**MEDIDAS DE PROTECCIÓN**
• Sistemas de apoyo • Registros de Clientes • Procesamiento en línea	Vital	ALTA ↑ Pérdida de ingresos Servicios a Clientes Decisiones de la Alta Dirección Costo de Reconstrucción Confidencialidad de Clientes ↓ BAJA	• Activar Hot Site • Respaldos • Plan de contingencias (probado cuatrimestral)
• Registros de Clientes • Base de datos Corporativa • Archivos legales • Proyectos de investigación • Control de procesos	Importante		• Sites alternos para procesamiento • Almacenamiento fuera del site • Actualizaciones diarias y semanales • Plan de contingencias (probado anual)
• Material de referencia • Información histórica (de 1 a 3 años) • Correspondencia departamental	Uso común		• Calendarios de retención • Cerraduras en lockers, escritorios y oficinas • Controles físicos y de medio ambiente
• Información histórica (mayor a 3 años)	No Esencial		• Precauciones normales

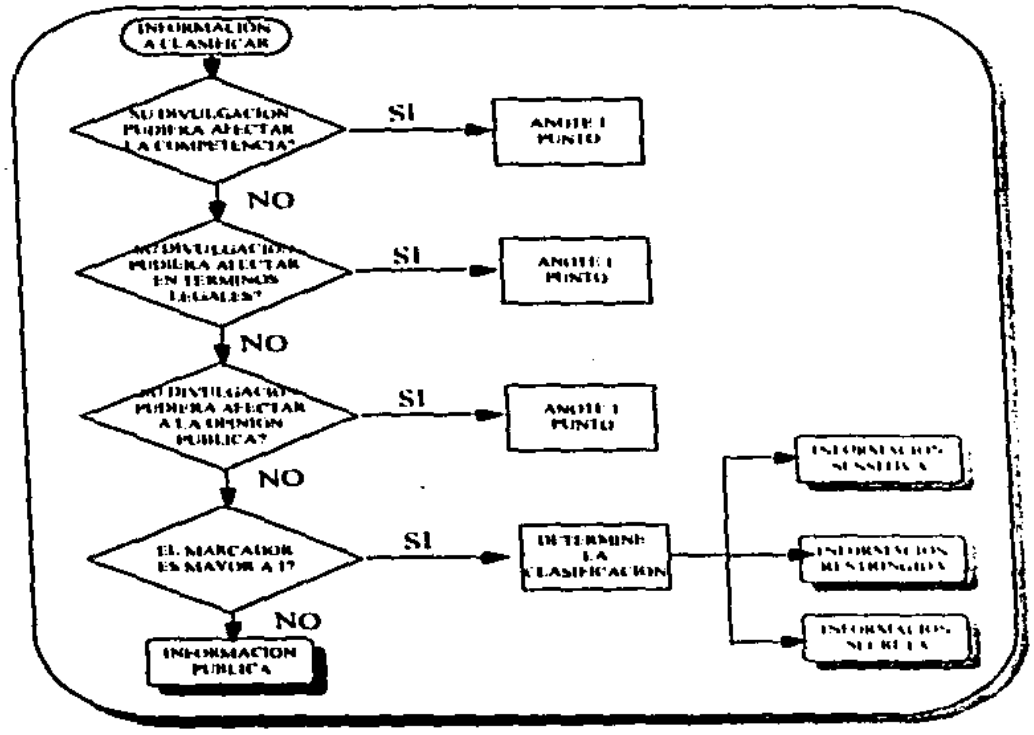
CLASIFICACIÓN POR INTEGRIDAD			
TIPO DE INFORMACIÓN	**CATEGORÍA**	**PÉRDIDA POTENCIAL**	**MEDIDAS DE PROTECCIÓN**
• Registros Financieros • Ministerio de Investigación • Sistema de reservaciones de Aerolíneas	Crítica	ALTA ↑ Fraude Exposición Financiera Decisiones de la Alta Dirección Registros incorrectos Confidencialidad de Clientes ↓ BAJA	• Encripción • Autentificación de mensajes • Doble Aprobación
• Sistemas de Procesamiento • Proyectos de Investigación • Base Corporativa de Datos • Registros del Personal	Sensitiva		• Identificadores individuales • Segregación de Responsabilidades • Verificación y Monitoreo • Programas para el control de cambios
• Custodia de registros • Directrices departamentales • Procedimientos Corporativos	Valiosa		• Acceso general basado en "necesidad de conocer" • Procedimientos de actualización y cambios • Principios de derechos de autor
• Directorio telefónico de la compañía	No Crítica		• Controles ordinarios del negocio

CLASIFICACIÓN POR CONFIDENCIALIDAD			
TIPO DE INFORMACIÓN	**CATEGORÍA**	**PÉRDIDA POTENCIAL**	**MEDIDAS DE PROTECCIÓN**
• Planes Estratégicos • Secretos del Negocio • Estrategias de Investigación	Registro Confidencial	ALTA ↑ Fraude Exposición Financiera Decisiones de la Alta Dirección Registros incorrectos Confidencialidad de Clientes ↓ BAJA	• Encripción • Asignación individual • Aislamiento de computadoras, sistemas y redes
• Datos Corporativos • Perfiles de Seguridad en el Acceso • Registros Personales • Propiedad de Software	Confidencial		• Autorización Individual • Acuerdos de no divulgación • Pistas de Auditoría • Escritorios, gabinetes y oficinas cerradas.
• Directrices Corporativas • Organigramas • Manuales de Procedimientos	Únicamente Uso Interno		• Acceso Interno • Necesidad de Conocer • Apropiado etiquetación
• Manuales y revistas	Publica		• Controles ordinarios del negocio

FLUJO PARA LA CLASIFICACIÓN DE INFORMACIÓN

El siguiente diagrama esquematiza un ejemplo, de manera general, de como se podría llegar a la clasificación de la información desde el punto de vista de Confidencialidad y además se recomienda que los resultados arrojados por la clasificación, se mantengan en una base de datos que indique la información o aplicación, su tipo de clasificación, desde que punto de vista se califica, quien es la autoridad para facultar el acceso y cuando se clasificó.

Debido a que el valor de la información no cambia continuamente, la clasificación deberá ser revisada periódicamente, por ejemplo cada año, y así determinar si se requieren nuevos cambios. *Cualquier cambio en su clasificación indicará también un cambio en las medidas de protección a la información.*



Existen varios beneficios derivados del proceso de clasificación de la información. El primero es que un programa de clasificación puede ayudar al desarrollo de políticas de protección por parte de los empleados y sus jefes además de que se comprometan en el uso apropiado de la información. La reacción de los empleados es favorable cuando la Administración Corporativa demuestra liderazgo y dirección, sin embargo, *la tarea de*

clasificar la información y sus niveles de protección deberá ser parte de la cultura de la organización. Adicionalmente, la categorización deberá sensibilizar a los empleados en la necesidad de proteger la información confidencial y respetar el derecho de privacia de sus compañeros.

Un segundo beneficio es que este programa claramente identificará la información esencial para la operación del negocio y podrá ayudar a motivar el desarrollo de un efectivo plan de contingencias. Adicionalmente, la identificación de información que es sensitiva a modificaciones, prepara al usuario final y al desarrollador del sistema, para seleccionar un apropiado control interno para asegurarse de la integridad de esa información. Un programa de clasificación de información también proporciona las bases para el análisis de la aplicaciones existentes y determinar cuales están adecuadamente protegidas.

SEGURIDAD INFORMÁTICA VS. AUDITORIA EN INFORMÁTICA

Seguridad informática es una función de reporte directo a la Dirección (nivel staff), responsable de recomendar, evaluar e implementar medidas de seguridad, mientras que la auditoria interna es una función de monitoreo independiente.

Ambos entes deberán trabajar de manera cercana compartiendo información de la siguiente manera:

- Un auditor deberá estar incluido en un comité de seguridad.
- Los auditores deberán revisar los procedimientos de seguridad antes de su implementación.
- Un miembro del staff de seguridad deberá apoyar a los auditores durante las auditorias en seguridad y participar con sus puntos de vista en cuanto a este rubro.

Las medidas de seguridad dentro de una organización pueden ser vistas como componentes dentro de su estructura de control interno y una efectiva función de auditoria interna como un potente monitoreador y analizador de la efectividad y apego a la seguridad.

Debido a que la seguridad en la información es una área de alto riesgo en cuanto a responsabilidad (reconocido por reguladores federales en EUA, personal certificado, dirección ejecutiva de corporaciones y auditores internos y externos), la función de seguridad es generalmente una labor de investigación por parte de los auditores. El administrador de la seguridad deberá estar involucrado con las técnicas de auditoria EDP (Electronic Data Processing) y anticiparse a los requerimientos que incluyan al ambiente de cómputo.

Tipicamente, los auditores EDP revisan los controles genéricos que integran la seguridad en los datos corporativos (por ejemplo, control de claves de acceso, controles de seguridad de usuarios finales, seguridad física sobre recursos críticos, y la habilitación de parámetros de seguridad en los archivos). Un auditor EDP no siempre detecta fraudes o discrepancias o direcciona todos los asuntos de seguridad; sin embargo, auditoría EDP deberá realizar sus revisiones y pruebas en las áreas importantes para asegurarse que el departamento de seguridad en informática está funcionando adecuadamente.

CAPITULO IV

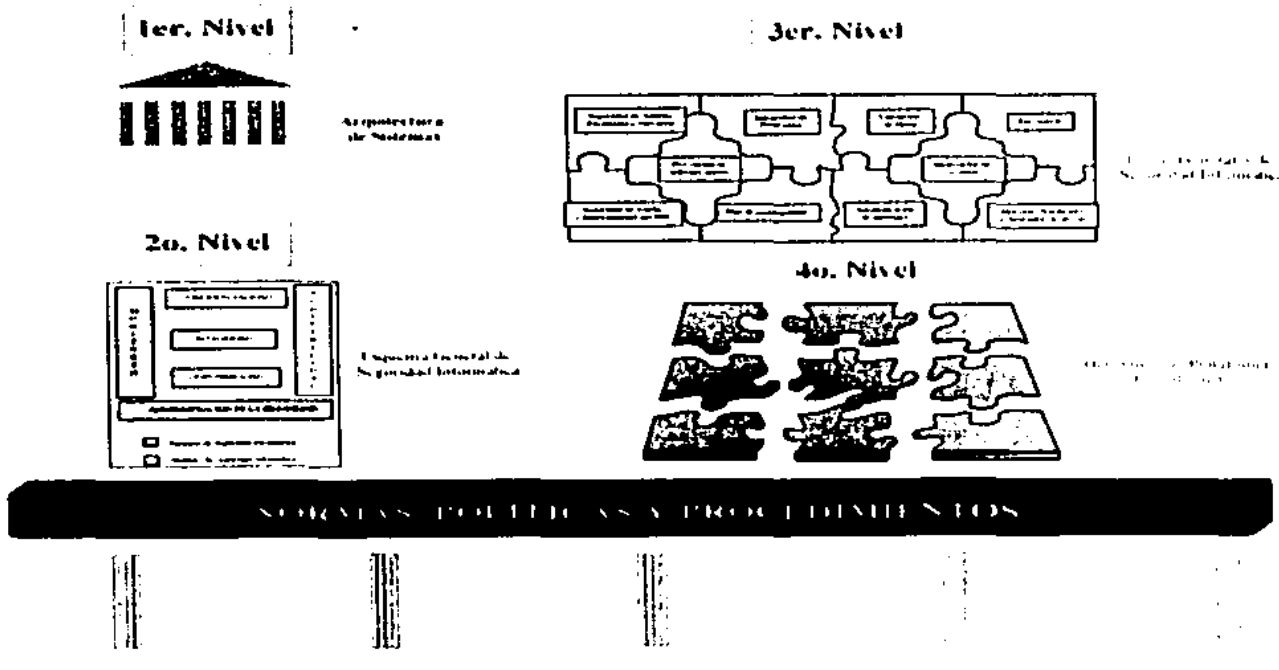
ESTRUCTURA DE SEGURIDAD

GENERALIDADES

El presente capitulo explica las piezas de seguridad a contemplar en un esquema general de sistemas logrando de manera adicional la estandarización de las medidas de seguridad que se deben incluir en dicho modelo.

El siguiente diagrama esquematiza los diferentes niveles de seguridad que se deberán presentar en cualquier organización que incluya la Función de Seguridad Informática; el primer nivel se refiere a la función o departamento de sistemas la cual contendra su estructura o arquitectura bien definida en cuanto a procesos, flujos de información, interfases, controles y validaciones, etc.; el segundo nivel muestra la integración de la función o departamento de Seguridad Informática representado por los atributos que forman su misión; en el tercer nivel se identifican las piezas o elementos de seguridad que deberá contemplar la función de S.I.[1] y del cual se tomará como punto de partida de este capitulo. El cuarto nivel es la traducción del tercer nivel (piezas o elementos) a herramientas, paquetes, esquemas operativos, etc.

Estos niveles deberán estar soportados y sustentados por normatividad, políticas, estándares, controles y procedimientos.



[1] Seguridad Informatica

PIEZAS GENERALES DE SEGURIDAD INFORMÁTICA

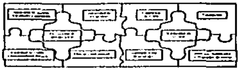
Las piezas de la Función de Seguridad Informática permiten, bajo un esquema tecnológico y funcional, considerar los atributos de seguridad y aplicarlos de manera precisa y tangible al modelo o estructura de sistemas traduciendolas en herramientas, estándares o esquemas operativos, cubriendo así, las necesidades de protección de la información y de los recursos tecnológicos para su procesamiento dentro de la Organización.

En general, las piezas son elementos o secciones que deberán incorporarse a la arquitectura de sistemas para la protección de la información.

Este tercer nivel está representado como un rompecabezas con lo cual se quiere representar que todas las piezas o elementos de seguridad están estrechamente ligadas y relacionadas entre sí. Cabe mencionar que la integración de estas piezas estará en función de la plataforma tecnológica en donde se este desarrollando y corriendo las aplicaciones, con esto se concluye que no todas las piezas tendrán participación en los esquemas de seguridad y que tampoco deberán llevar un orden estricto en su implantación, el orden será determinado conforme a los resultados que arroje un análisis o diagnóstico de riesgos (del cual se hablará en el capitulo VI).

El objetivo y funciones de cada una de las piezas se explicará en las siguientes páginas; el esquema representa las funciones de cada pieza.

3er. Nivel



SEGURIDAD DE ACCESO, FACULTADES Y SERVICIOS

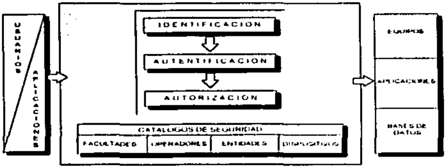
OBJETIVO DE LA PIEZA

Controlar el acceso a los recursos informáticos y a la información, de tal manera que únicamente se permita el uso y afectación de la información a los entes autorizados.

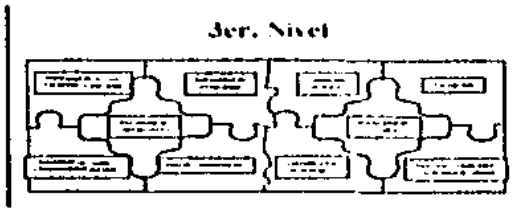
FUNCIONES

- **Distinguir al solicitante como un ente previamente autorizado.**
- **Asegurar que el solicitante activado es el legítimo.**
- **Autorizar el uso a los recursos informáticos y datos a los usuarios facultados de acuerdo con su responsabilidad.**
- **Registrar los eventos realizados y dar seguimiento a las situaciones de excepción.**
- **Apoyar a la administración de los catálogos, recursos y atributos de la pieza de seguridad.**

ESQUEMA



El cuarto nivel de seguridad estará apoyado con software para el control de usuarios en donde permita especificar o limitar los acceso a las aplicaciones, bases de datos, recursos, dispositivos y equipos por medio de identificadores de usuario (users-id) y sus claves de acceso (password).



INTEGRIDAD DE PROGRAMAS

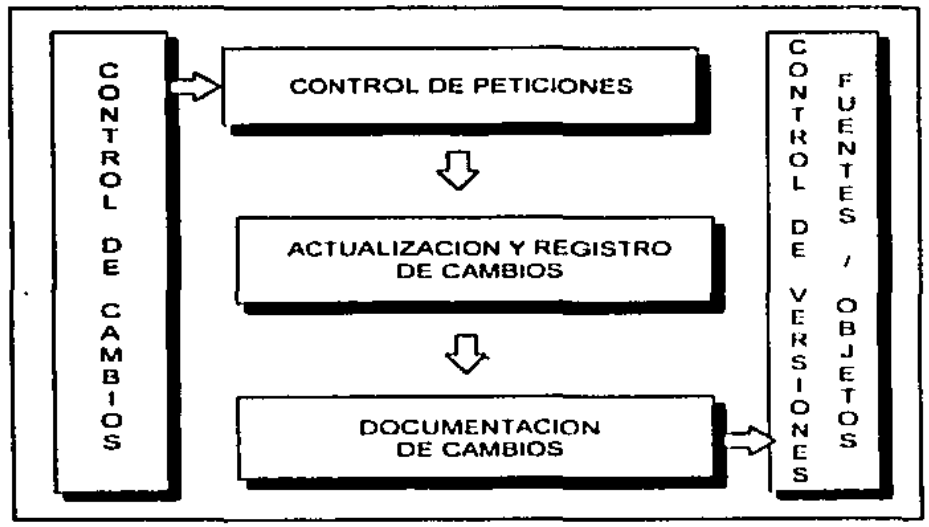
OBJETIVO DE LA PIEZA:

Controlar la actualización y modificación de software (software de infraestructura y programas de aplicación) a fin de mantener su consistencia, integridad y disponibilidad.

FUNCIONES

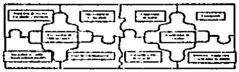
- Controlar las sesiones de cambio a código fuente y objeto.
- Proteger las versiones de producción y permitir cambios en las versiones de prueba.
- Garantizar la consistencia en el manejo de versiones.
- Documentar las actualizaciones hechas al software.
- Verificar que las actualizaciones de programas liberados a producción correspondan con las versiones autorizadas.

ESQUEMA



El cuarto nivel de seguridad estará apoyado con procedimientos manuales o una herramienta automatizada que permita mantener un control y administración de cambios, de peticiones y de versiones de software así como de programas fuentes y objetos.

4er. Nivel



4.3.1 VALIDACIÓN DE DATOS

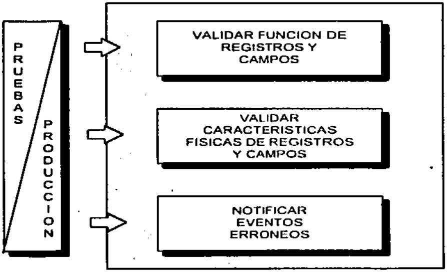
OBJETIVO DE LA PIEZA:

Validar que en el ambiente de pruebas y producción previo a su proceso los datos cumplan con las características predefinidas en la aplicación.

FUNCIONES

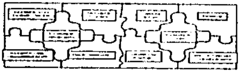
- **Verificar que el contenido de los campos corresponda a los rangos definidos para cada tipo de dato.**
- **Validar la correcta aplicación de las características físicas de los registros y campos (longitud y tipo).**
- **Rechazar y notificar los registros que no cumplan con las características predefinidas.**
- **Manejar estadísticas de información propia de la pieza para su análisis.**

ESQUEMA



El cuarto nivel deberá estar apoyado por esquemas operativos por parte de los desarrolladores y por parte de una función de Pruebas y Afinación de la Aplicación en Ambiente de Desarrollo previo a la liberación a un ambiente de producción que se encargaran de realizar todas las validaciones pertinentes.

Jer. Nivel



ENCRIPCIÓN

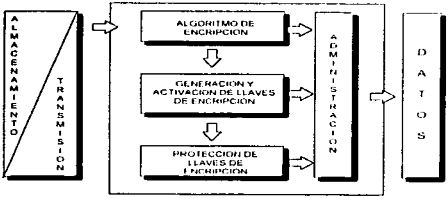
OBJETIVO DE LA PIEZA:

Garantizar que la información que viaje a través de la red de comunicaciones y aquélla contenida en los diferentes medios de almacenamiento se mantenga confidencial e íntegra, de tal manera que sólo pueda ser accesada por aquellos entes (usuarios, aplicaciones o departamentos) autorizados.

FUNCIONES

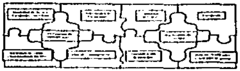
- **Generación de llaves de encripción a través de algoritmos aleatorios.**
- **Proteger la confidencialidad y autenticidad de los mensajes y datos que viajan a través de la red de comunicaciones y/o se almacenan en diversos dispositivos.**
- **Administrar la asignación, custodia y distribución de las llaves de encripción con los entes facultados.**
- **Mantener respaldos de las llaves de encripción dentro de mecanismos seguros.**
- **Borrar y actualizar llaves de encripción en caso de violación.**
- **Proteger el ruteo de mensajes a través de la red.**

ESQUEMA



El cuarto nivel de seguridad podrá estar representado por herramientas de software y/o hardware de encripción de datos.

3er. Nivel



AUTENTIFICACION DE MENSAJES

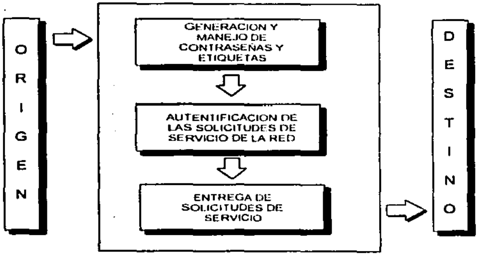
OBJETIVO DE LA PIEZA

Asegurar que las solicitudes de servicio que viajen a través de la red de comunicaciones de la Organización sean auténticos.

FUNCIONES

- Generar contraseñas y etiquetas de protección e identificación de mensajes.
- Controlar contraseñas y etiquetas.
- Verificar la validez de usuarios y servidores autorizados.
- Certificar el ciclo de envío y recepción de mensajes.
- Registro de eventos para detección de situaciones de afectación de mensajes.

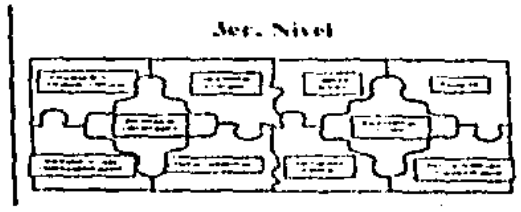
ESQUEMA



El cuarto nivel puede ser cubierto con herramientas de software y/o hardware como son el Kerberos[2] y los Firewalls[3] que su objetivo es el de autentificar mensajes, usuarios y servidores.

---

[2] Ver Glosario
[3] Ver Glosario



PREVENCIÓN CONTRA SOFTWARE NOCIVO

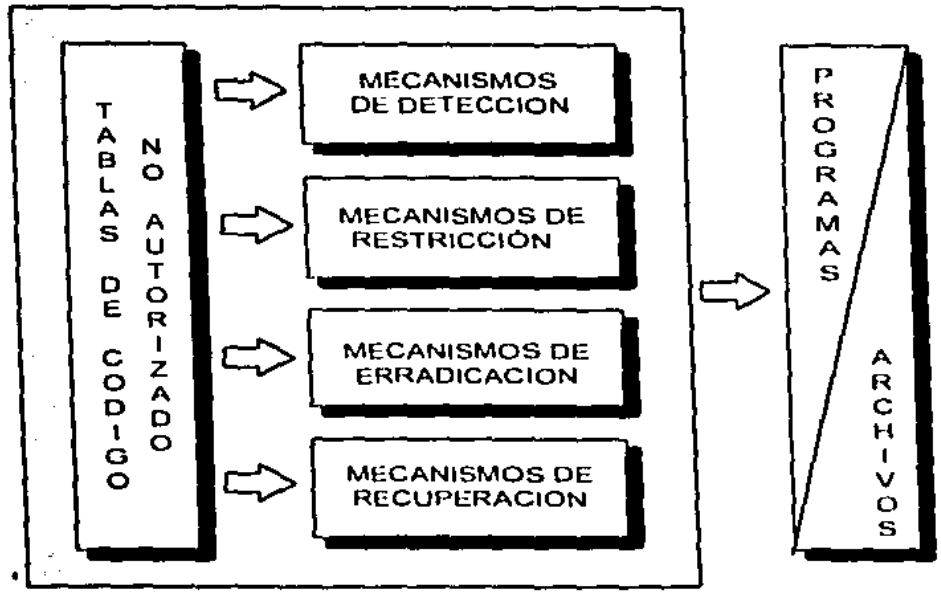
OBJETIVO DE LA PIEZA:

Asegurar que los programas y archivos no sean contaminados y/o afectados por código no autorizado, así como evitar la ejecución no autorizada de rutinas de alto riesgo que afecten la integridad de la información y los procesos.

FUNCIONES

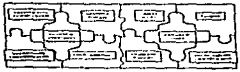
- Validar que la información y los programas que se introducen en el sistema no contengan código no autorizado.
- Validar comportamiento de los programas.
- Detectar y en su caso notificar existencia de código no autorizado.
- Aislar y eliminar código no autorizado.
- Evitar la ejecución de programas no autorizados.
- Reparar y dejar información y programas en estado valido.
- Actualizar tablas de validación de código no autorizado.

ESQUEMA



Las vacunas, software anti-virus y programas de detección de rutinas o comandos de alto riesgo son los mecanismos que aplicarían para el cuarto nivel en la seguridad.

4er. Nivel



SEGURIDAD EN LA CONFIGURACIÓN Y FUNCIONALIDAD DEL HARDWARE

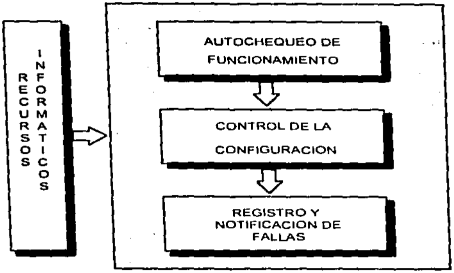
OBJETIVO DE LA PIEZA:

Asegurar la funcionalidad y confiabilidad del hardware utilizado para la operación de procesos.

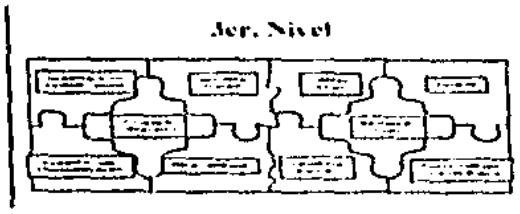
FUNCIONES

- **Aviso del estado del deterioro de los componentes físicos.**
- **Restringir los acceso a los parámetros y/o elementos físicos de configuración del hardware.**
- **Verificar de manera automática el correcto funcionamiento de las piezas de hardware.**
- **Llevar una bitácora de fallas y problemas propios del hardware.**
- **Balanceo y distribución automático de cargas de operación.**

ESQUEMA



Una herramienta automatizada junto con procedimientos manuales deberán apoyar la implantación de esta pieza representada como el cuarto nivel en la seguridad. Este conjunto deberá cumplir con las funciones y en general con lo especificado en el esquema.



PLAN DE CONTINGENCIAS

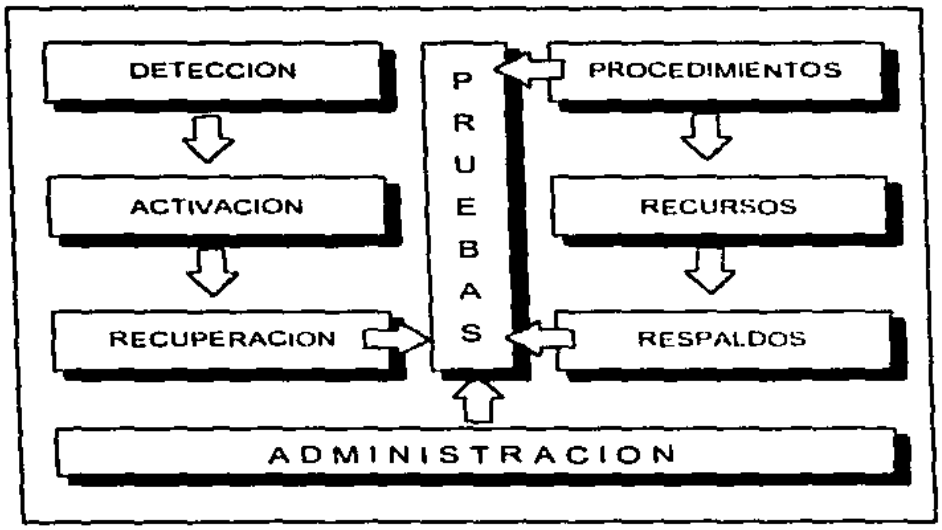
OBJETIVO DE LA PIEZA

Asegurar la continuidad y disponibilidad de los servicios, recursos informaticos y de communicaciones utilizados por el personal y clientes de la Organización, ante la presencia de eventos imprevisibles.

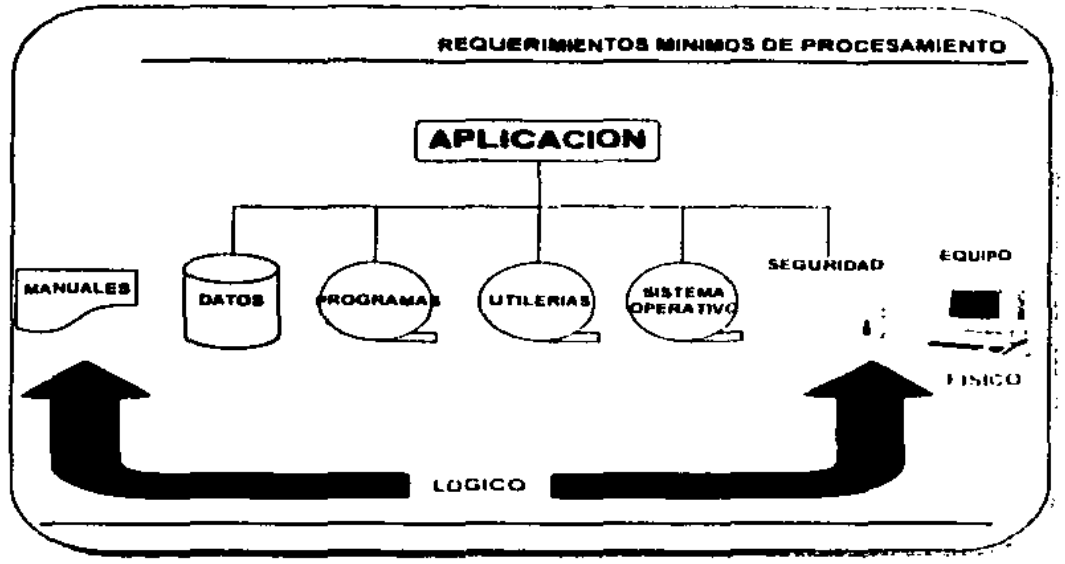
FUNCIONES

- Definición de prioridades de atención.
- Control de respaldos.
- Documentación de procedimientos de planes de contingencias.
- Control de los recursos para planes de contingencia.
- Desarrollo de pruebas y simulacros.
- Evaluación del impacto de las contingencias ocurridas.
- Generación de estadisticas de eventos.
- Restablecimiento de la operación normal.

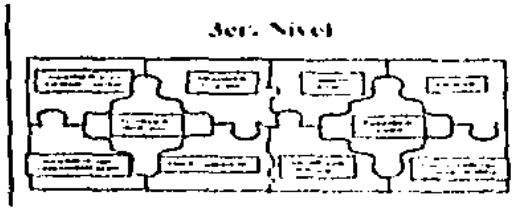
ESQUEMA



El cuarto nivel de seguridad puede ser implantado con ayuda de paquetes comerciales apoyados de procedimientos operativos y una buena definición de roles y responsabilidades para cada uno de los participantes aplicables cuando se presente una contingencia.



La figura anterior muestra los elementos necesarios para la recuperación del servicio automatizado en caso de una contingencia. Por un lado los aspectos lógicos como son los manuales y procedimientos, los programas fuentes y objetos, las utilerías, el sistema operativo, los esquemas de seguridad y lo más importante son los datos ya que sin éstos no servirá de nada el levantar un ambiente de emergencia si no existen datos o información a procesar. Por otro lado se encuentran los aspectos físicos como son el elemento humano y el equipo donde se procesará.



RASTREADOR DE EVENTOS SIGNIFICATIVOS DE SEGURIDAD

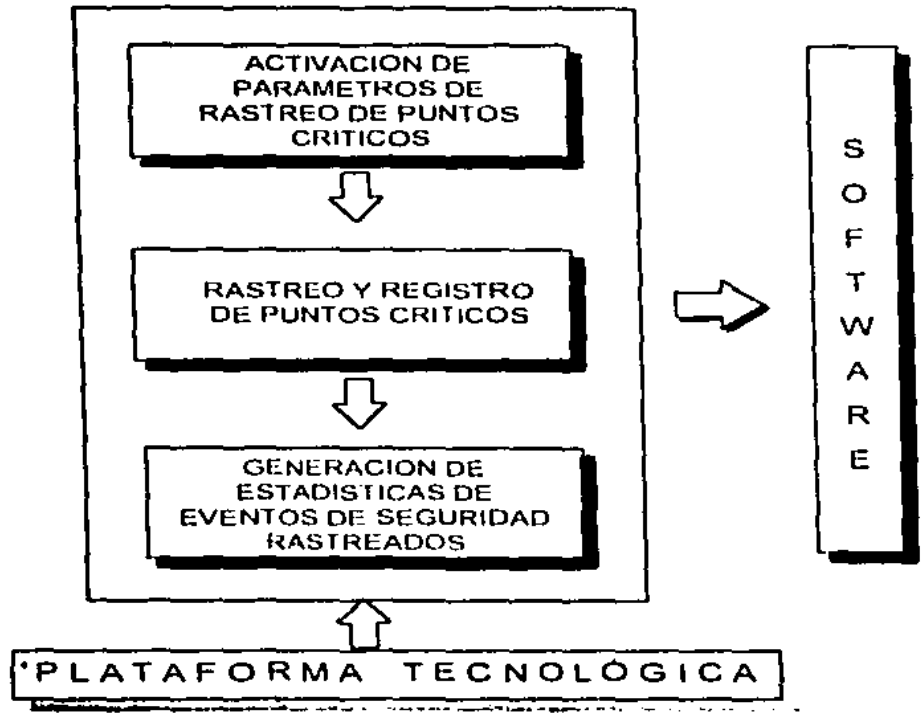
OBJETIVO DE LA PIEZA:

Indagar, marcar y llevar registro de aspectos relevantes predefinidos que pueden afectar la seguridad.

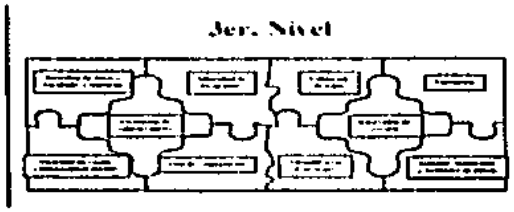
FUNCIONES

- Identificar y activar parámetros de seguridad en los puntos críticos de los procesos a dar seguimiento.
- Rastrear y registrar el comportamiento en puntos críticos seleccionados.
- Generar reportes de eventos significativos y de excepción para su análisis y toma de decisiones.
- Actualizar parámetros según prioridades y comportamiento histórico.

ESQUEMA



Elementos o herramientas que pueden considerarse en el cuarto nivel son las bitácoras o logs de seguridad, pistas de auditoría y el software de seguridad que integran en algunas plataformas, al sistema operativo.



DETECTOR, NOTIFICADOR Y ACTIVADOR DE ALERTAS DE SEGURIDAD

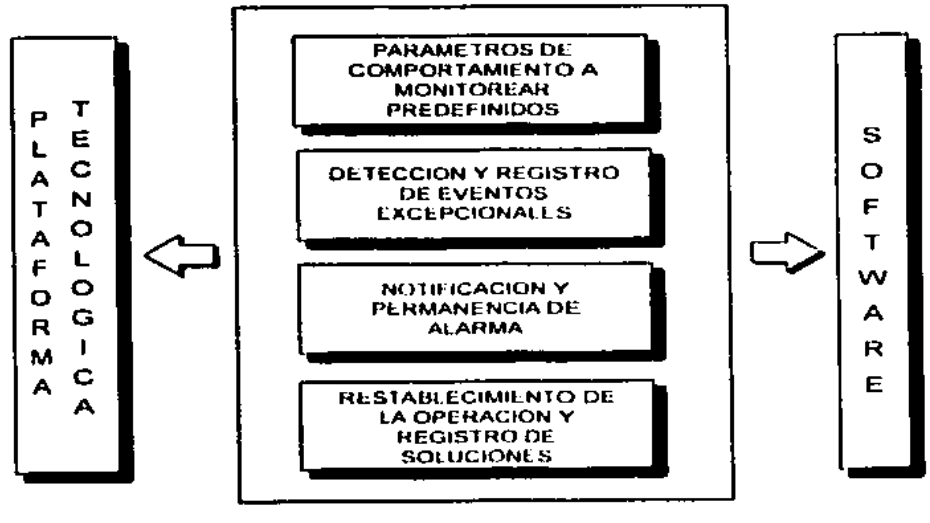
OBJETIVO DE LA PIEZA

Detectar y registrar eventos de seguridad que estén fuera de los parámetros normales previamente establecidos, así como notificar la situación a las entidades responsables.

FUNCIONES

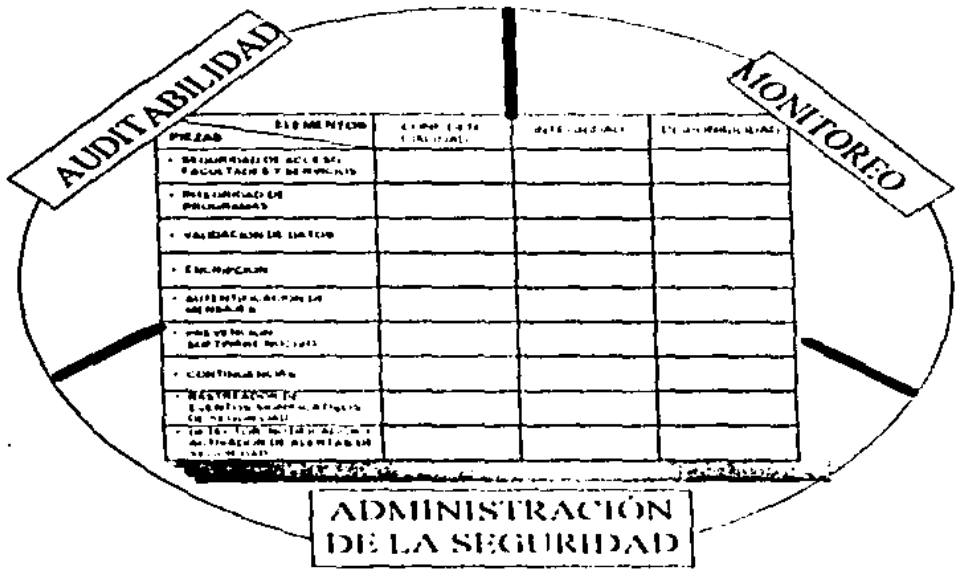
- Detección y registro de excepciones de seguridad de acuerdo con los parámetros y límites establecidos.
- Registro de intentos de acceso tanto exitosos como fallidos.
- Notificación inmediata de eventos ocurridos a las entidades responsables.
- Registro de soluciones a los eventos ocurridos.
- Verificación de límites y actualización automática de parámetros de seguridad si se requiere.
- Generación de estadísticas de eventos ocurridos.

ESQUEMA

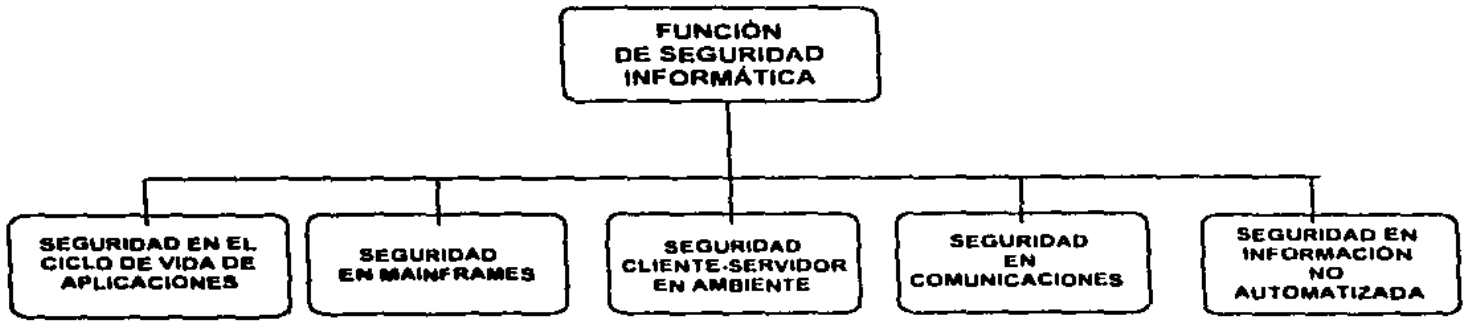


El cuarto nivel de seguridad podrá ser cubierto por el software de seguridad de cada una de las plataformas o, en su caso, de desarollos a la medida que cumplan con las funciones de la pieza.

CONTRIBUCIÓN DE LAS PIEZAS DE SEGURIDAD EN LA PROTECCIÓN DE LOS ATRIBUTOS DE LA INFORMACIÓN.



El sombreado de la matriz nos indica con que piezas podremos cubrir o proteger los diferentes atributos de la información desde la perspectiva de seguridad; está matriz está reforzada con la cobertura de las funciones de auditoria, el monitoreo de eventos y la administración de la seguridad.



Este diagrama propone que la Función de Seguridad Informática integre a su vez, cinco actividades o procesos de los cuales se explicará el propósito de cada uno de ellos así como los puntos o indicadores de seguridad que deberán considerarse en las diferentes áreas tecnológicas dentro de la organización.

SEGURIDAD EN EL CICLO DE VIDA DE LAS APLICACIONES

PROPÓSITO:

Incorporar niveles de seguridad en el ciclo de vida de las aplicaciones, así como en los procesos y herramientas utilizadas durante:

ETAPAS DE DESARROLLO

- Análisis o Concepción de la Aplicación
- Diseño
- Construcción
- Pruebas, Afinación y Cambios
- Liberación a Producción

Ó

ETAPAS DE ADQUISICIÓN

- Perfil de aplicación requerida
- Identificación y Selección
- Pruebas y Afinación en desarrollo ccon el proveedor
- Adquisicion del software

ETAPAS DE CAMBIOS Y OPTIMIZACIONES

- Solicitud de cambios, correcciones y optimizaciones
- Programación
- Pruebas y Afinación
- Liberación a Producción

ETAPAS DE DESARROLLO

Los procesos de seguridad que deberán considerarse en la etapa del desarrollo de aplicaciones estarán dispersas dentro de sus tres etapas:

En la primer etapa que es el *Análisis o Concepción de la Aplicación* se tomaran en cuenta aspectos como la seguridad en datos que, aislados o al integrar la información, puedan ser considerados como sensitivos, es decir, de alto riesgo para la organización; se deberán determinar sus mecanismos de validación y las reglas para establecer vistas de acceso a los mismos para los usuarios facultados, así como las medidas de protección del esquema de base de datos correspondiente.

Estos datos deberán analizarse desde su forma de alimentación a las aplicaciones ya sean por transacciones en línea, en batch vía cintas, disquetes, de manera verbal, etc., y es aquí donde participa otro aspecto de seguridad en acceso y facultades el cual deberá definir los criterios para determinar que áreas y usuarios

podrán tener acceso a la aplicación así como las transacciones que podrán realizar (quien entra y que puede hacer); se deberá considerar el hecho de elaborar procedimientos para reautentificación en las transacciones sensitivas que así lo requieran.

Una vez que se analizan entradas y procesos, toca ahora introducir la parte de seguridad en la información no automatizada, es decir, aquella información que genera la aplicación en diferentes medios (papel, voz, terminales, dispositivos magnéticos, etc.) y de la cual hablaré más adelante.

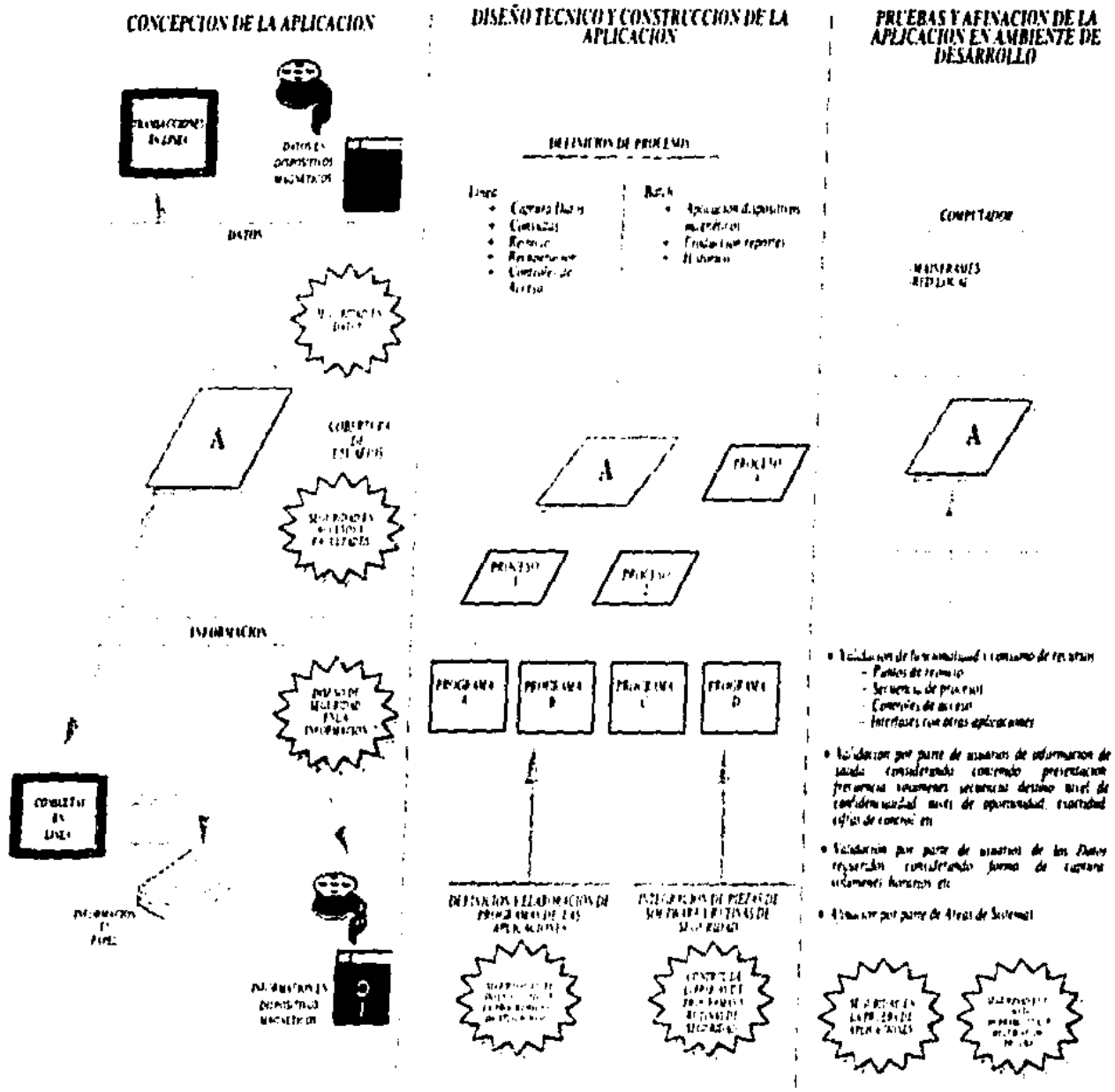
En la siguiente etapa de *Diseño y Construcción* los aspectos de seguridad a tomar en cuenta están relacionados con la seguridad en el diseño técnico y programación de aplicaciones en donde se deberán determinar las medidas de seguridad a contemplar en el diseño de las aplicaciones en sus entradas, procesos, consultas y salidas; se deberán seleccionar también las rutinas de programación o algoritmos de seguridad que permitan la protección y el análisis de los programas de las aplicaciones así como la determinación de los puntos de validación intermedios en el proceso de programación y el desarrollo de pistas de auditoria.
También se deberán determinar los tipos de pruebas de escritorio para asegurar que los procesos ofrecen integridad en el manejo de los datos e información, así como el seguimiento y certificación de la realización de dichas pruebas.
Dentro del control de librerías de programas y rutinas de seguridad se deberán determinar aquellas rutinas de seguridad que se incorporaran a los programas, se deberán especificar las reglas para la validación de datos, generación de cifras de control, el control de acceso y facultades y la validación de rutinas de alto riesgo. Así mismo de definirán las medidas de protección y distribución de copias de librerías y piezas de software.

En la tercera etapa que es la de *Pruebas y Afinación* antes de liberar a producción, la seguridad en la prueba de aplicaciones deberá incluir las reglas para las pruebas de las aplicaciones definiendo los datos pruebas (para protección de su confidencialidad), pruebas de volumen y funcionalidad total; se deberán establecer los criterios para la documentación del desarrollo y resultados de las pruebas y determinar también los procedimientos para validar las pistas de auditoria y certificar la realización de las pruebas.
La parte de seguridad en el uso de herramientas y control de pruebas deberá contener las políticas y medidas de seguridad para separar el ambiente de prueba del ambiente de producción, las medidas de protección de la confidencialidad de los datos utilizados en las pruebas de las aplicaciones. En caso de ser necesario se deberá seleccionar y coordinar la implantación de medidas de seguridad para la protección de herramientas y recursos de pruebas.

También se debera definir los esquemas para el control de versiones y la protección contra emisión no autorizada de copias de las aplicaciones no propietarias.

El siguiente diagrama ilustra lo anterior.

SEGURIDAD EN EL CICLO DE VIDA DE LAS APLICACIONES
- Desarrollo



ETAPAS DE ADQUISICION

Cuando sea necesario que una aplicación sea desarrollada por personal externo a la organización, en la etapa de *Identificación y Selección de la Aplicación Requerida* se deberán considerar los aspectos relacionados con la seguridad en el diseño técnico y programación de aplicaciones en donde se deberán determinar las medidas de seguridad a contemplar en el diseño de las aplicaciones en sus entradas, procesos, consultas y salidas; se deberán seleccionar también las rutinas de programación o algoritmos de seguridad que permitan la protección y el análisis de los programas de las aplicaciones así como la determinación de los puntos de validación intermedios en el proceso de programación y el desarrollo de pistas de auditoria[4] .

También se deberán determinar los tipos de pruebas de escritorio para asegurar que los procesos ofrecen integridad en el manejo de los datos e información, así como el seguimiento y certificación de la realización de dichas pruebas.

Dentro del control de librerías de programas y rutinas de seguridad se deberán determinar aquellas rutinas de seguridad que se incorporaran a los programas, se deberán especificar las reglas para la validación de datos, generación de cifras de control, el control de acceso y facultades y la validación de rutinas de alto riesgo. Así mismo de definirán las medidas de protección y distribución de copias de librerías y piezas de software.

En la tercera etapa que es la de *Pruebas y Afinación de la Aplicación en ambiente de Desarrollo con participación del Proveedor*, la seguridad en la prueba de aplicaciones deberá incluir las reglas para las pruebas de las aplicaciones definiendo los datos pruebas (para protección de su confidencialidad), pruebas de volumen y funcionalidad total; se deberán establecer los criterios para la documentación del desarrollo y resultados de las pruebas y determinar también los procedimientos para validar las pistas de auditoria y certificar la realización de las pruebas.

La parte de seguridad en el uso de herramientas y control de pruebas deberá contener las políticas y medidas de seguridad para separar el ambiente de prueba del ambiente de producción, las medidas de protección de la confidencialidad de los datos utilizados en las pruebas de las aplicaciones. En caso de ser necesario se deberá seleccionar y coordinar la implantación de medidas de seguridad para la protección de herramientas y recursos de pruebas.

También se deberá definir los esquemas para el control de versiones y la protección contra emisión no autorizada de copias de las aplicaciones no propietarias.

En la ultima etapa *Adquisición de la Aplicación* se deberá incluir la seguridad en los convenios con terceros en donde se definirán los criterios para que las nuevas adquisiciones cumplan con las cláusulas de

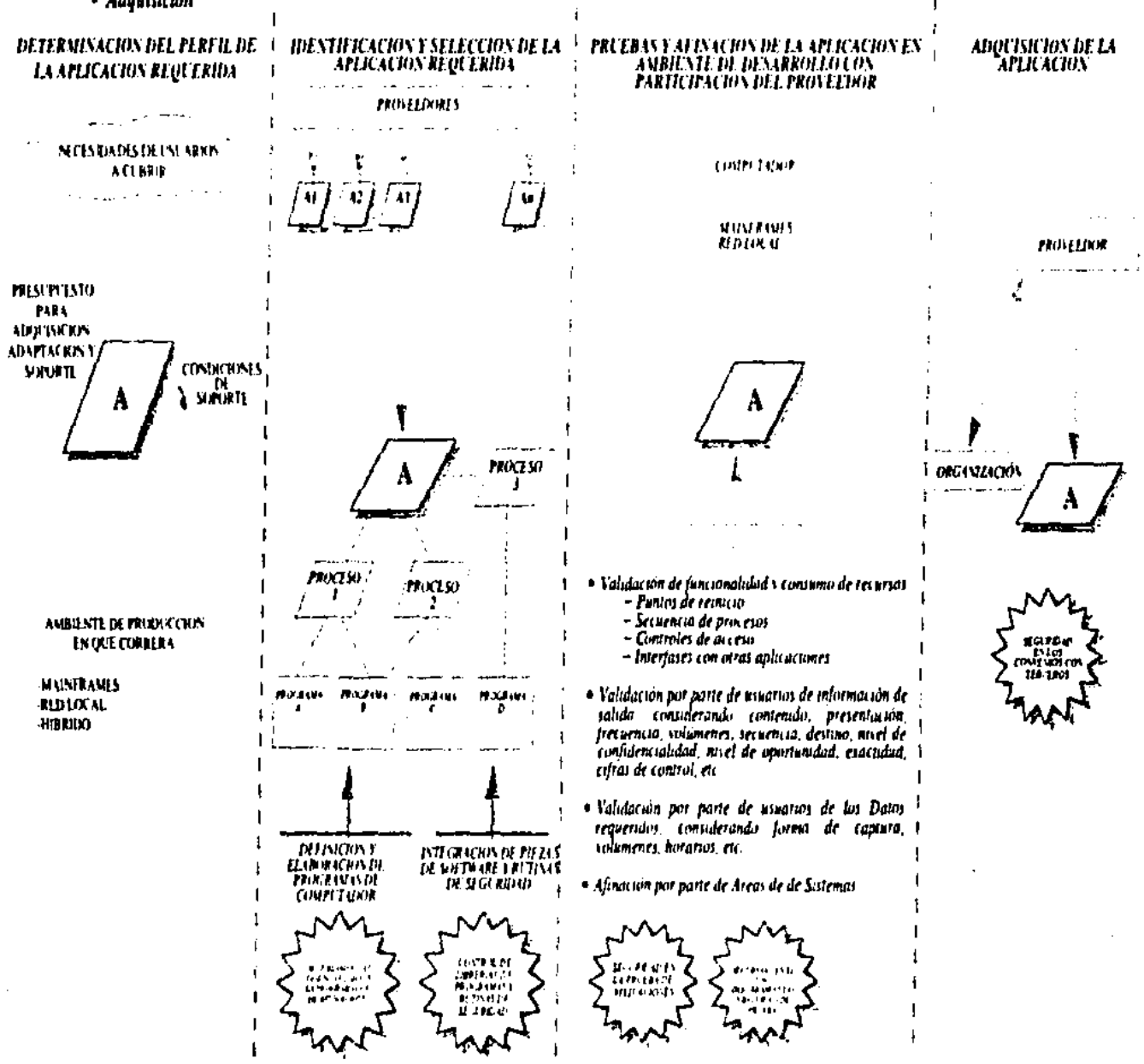
[4] Ver Glosario

confidencialidad, derechos patrimoniales y medidas de seguridad internas; se deberán determinar los procedimientos para certificar que las nuevas adquisiciones cumplen con las políticas y reglamentos de seguridad para el desarrollo y mantenimiento de aplicaciones así como incluir en los convenios con terceros, disposiciones que garanticen la propiedad y confidencialidad de la información.

La siguiente figura esquematiza lo anterior:

SEGURIDAD EN EL CICLO DE VIDA DE LAS APLICACIONES

- *Adquisición*



ETAPAS DE CAMBIOS Y OPTIMIZACIONES

Cuando se requieran modificaciones a la aplicación o programas, en la etapa *de programación de cambios, correcciones y optimizaciones*, deberá participar seguridad en cambios a las aplicaciones en la cual se deberá especificar los criterios para incorporar los puntos de control de seguridad en los cambios realizados, determinar controles de acceso y pistas de auditoria para proteger los archivos y las librerías de programas, así como asegurarse de la existencia y uso de controles para la verificación de la consistencia de código fuente contra la de código objeto.

La seguridad en el diseño técnico y programación de aplicaciones, como anteriormente se ha mencionado, deberá determinar las medidas de seguridad a contemplar en el diseño de las aplicaciones en sus entradas, procesos, consultas y salidas; se deberán seleccionar también las rutinas de programación o algoritmos de seguridad que permitan la protección y el análisis de los programas de las aplicaciones así como la determinación de los puntos de validación intermedios en el proceso de programación y el desarrollo de pistas de auditoria.

También se deberán determinar los tipos de pruebas de escritorio para asegurar que los procesos ofrecen integridad en el manejo de los datos e información, así como el seguimiento y certificación de la realización de dichas pruebas.

Dentro del control de librerías de programas y rutinas de seguridad se deberán determinar aquellas rutinas de seguridad que se incorporaran a los programas, se deberán especificar las reglas para la validación de datos, generación de cifras de control, el control de acceso y facultades y la validación de rutinas de alto riesgo. Así mismo de definirán las medidas de protección y distribución de copias de librerías y piezas de software.

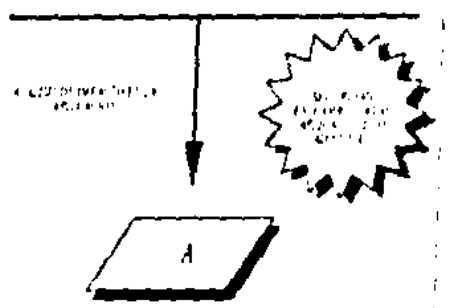
En la parte de *pruebas y afinación de la aplicación en ambiente de desarrollo*, la seguridad en la prueba de aplicaciones deberá incluir las reglas para las pruebas de las aplicaciones definiendo los datos pruebas (para protección de su confidencialidad), pruebas de volumen y funcionalidad total; se deberán establecer los criterios para la documentación del desarrollo y resultados de las pruebas y determinar también los procedimientos para validar las pistas de auditoria y certificar la realización de las pruebas.

La parte de seguridad en el uso de herramientas y control de pruebas deberá contener las políticas y medidas de seguridad para separar el ambiente de prueba del ambiente de producción, las medidas de protección de la confidencialidad de los datos utilizados en las pruebas de las aplicaciones. En caso de ser necesario se deberá seleccionar y coordinar la implantación de medidas de seguridad para la protección de herramientas y recursos de pruebas.

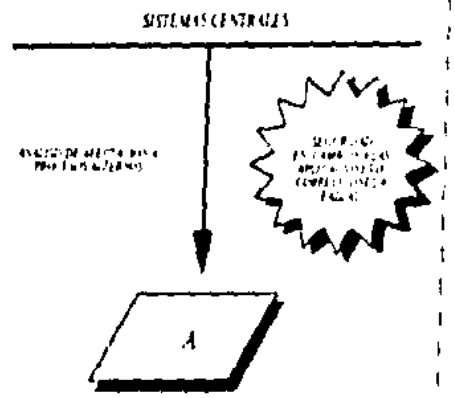
También se deberá definir los esquemas para el control de versiones y la protección contra emisión no autorizada de copias de las aplicaciones no propietarias. La figura siguiente lo ilustra.

SEGURIDAD EN EL CICLO DE VIDA DE LAS APLICACIONES
- Cambios, correcciones y optimizaciones

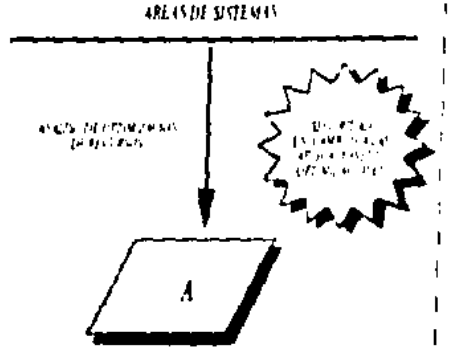
CAMBIOS SOLICITADOS POR USUARIOS



CORRECCIONES POR FALLAS EN PRODUCCION

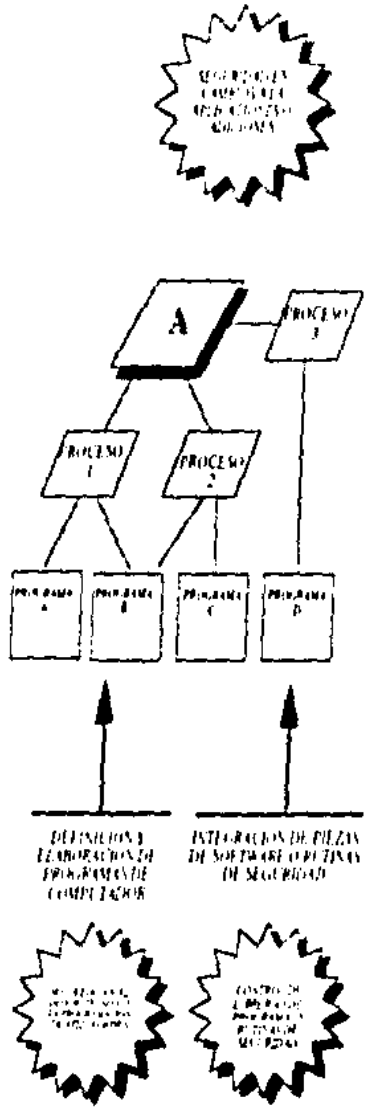


OPTIMIZACIONES A LA APLICACION EN EL USO DE LOS RECURSOS DE COMPUTO

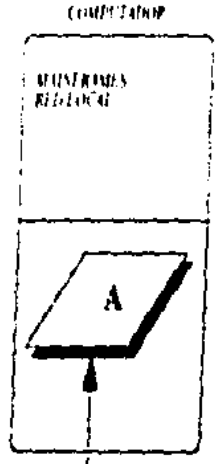


PROGRAMACION DE CAMBIOS, CORRECCIONES Y OPTIMIZACIONES

INTEGRACION DE CAMBIOS, CORRECCIONES Y OPTIMIZACIONES EN LOS PROCESOS Y EN LOS PROGRAMAS



PRUEBAS Y AFINACION DE LA APLICACION EN AMBIENTE DE DESARROLLO



- Validacion de funcionalidad y consumo de recursos
  - Puntos de reinicio
  - Secuencia de procesos
  - Controles de acceso
  - Interfases con otras aplicaciones
  - cifras de control de procesos
- Validacion por parte de usuarios de información de salida considerando contenido presentación, frecuencia, volumenes secuencia destino nivel de confidencialidad nivel de oportunidad exactitud, cifras de control etc
- Validacion por parte de usuarios de los Datos capturados considerando forma de captura, volumenes horarios etc
- Afinacion por parte de Areas de Sistemas

SEGURIDAD EN MAINFRAMES

PROPÓSITO:

Establecer y fortalecer los niveles de seguridad en la custodia, procesamiento y distribución de la información, así como en los procesos, aplicaciones y dispositivos magnéticos.

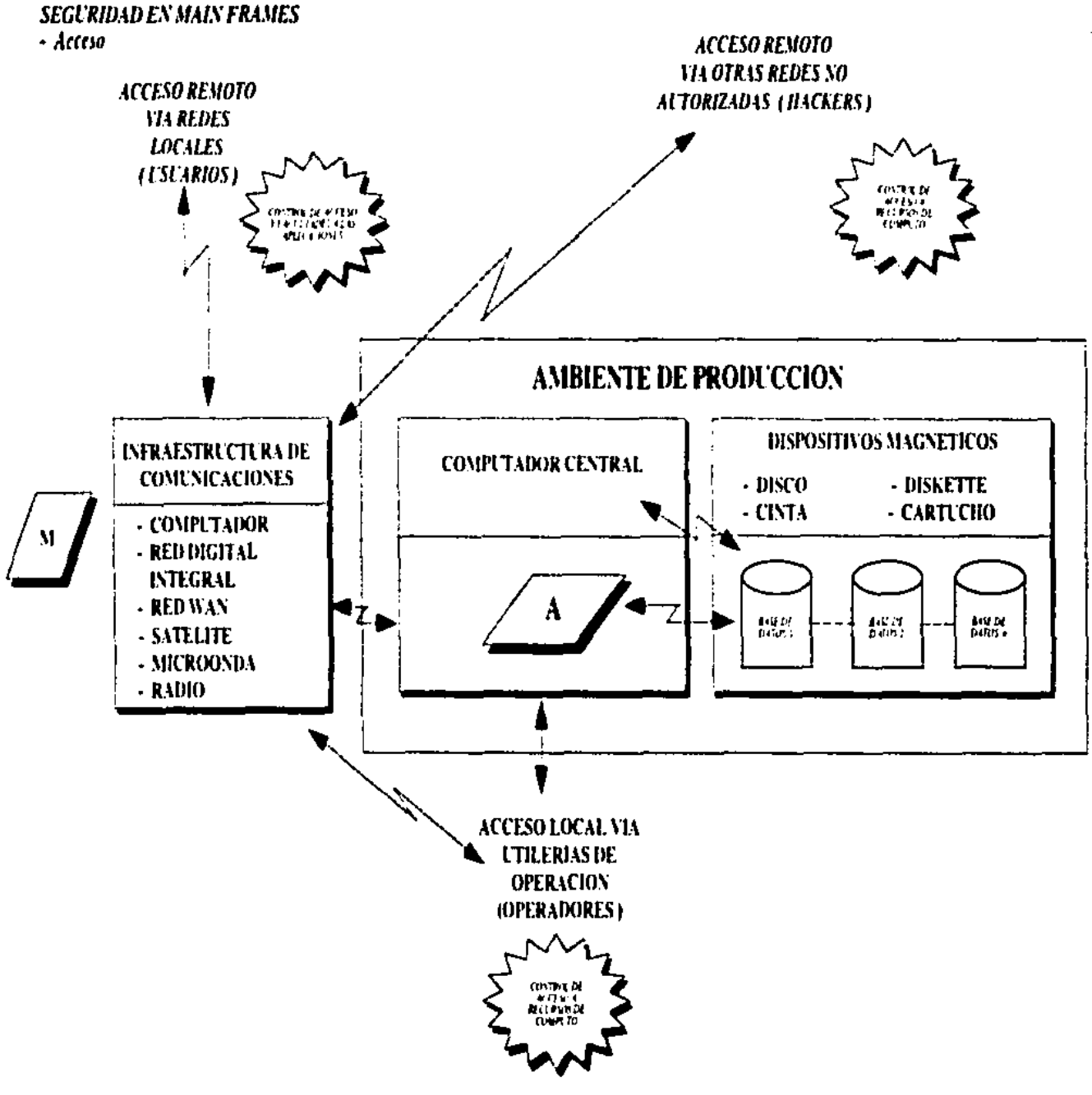
RESPONSABILIDADES DEL PROCESO:

- Establecer un control de acceso a los equipos mainframes así como a los dispositivos magnéticos.
- Seguridad en la configuración y parametrización del software propio del equipo de cómputo.
- Administración de cambios, pruebas y liberación de aplicaciones.
- Seguridad en la operación y ejecución de procesos.
- Monitoreo y auditabilidad en la operación del equipo de cómputo.
- Planes de contingencia ante casos de desastre.
- Control de medios y dispositivos magnéticos.

ACCESO

El acceso remoto de otras redes ya sean internas o externas a la organización, deberán cumplir con la parte de control de acceso y facultades a las aplicaciones la cual deberá establecer controles confiables de identificación y autentificacion de usuarios, así como verificación de controles de acceso y facultades (quien entra y a que) en aplicaciones y software de infraestructura de redes locales.

Toda la parte de datos de producción que corran bajo ambientes mainframes, deberán mantener un control de acceso a sistemas centrales a los recursos de computo los cuales deberán mantener un control de acceso y autorización en el uso de recursos de computo y bases de datos, esquemas de monitoreo y seguimiento a situaciones de excepción de eventos de seguridad e implantacion de los controles correspondientes.


SEGURIDAD EN MAIN FRAMES
- Acceso
ACCESO REMOTO VIA REDES LOCALES (USUARIOS)
ACCESO REMOTO VIA OTRAS REDES NO AUTORIZADAS (HACKERS)
AMBIENTE DE PRODUCCION
INFRAESTRUCTURA DE COMUNICACIONES
- COMPUTADOR
- RED DIGITAL INTEGRAL
- RED WAN
- SATELITE
- MICROONDA
- RADIO
M
COMPUTADOR CENTRAL
A
DISPOSITIVOS MAGNETICOS
- DISCO
- DISKETTE
- CINTA
- CARTUCHO
ACCESO LOCAL VIA UTILERIAS DE OPERACION (OPERADORES)

OPERACIÓN

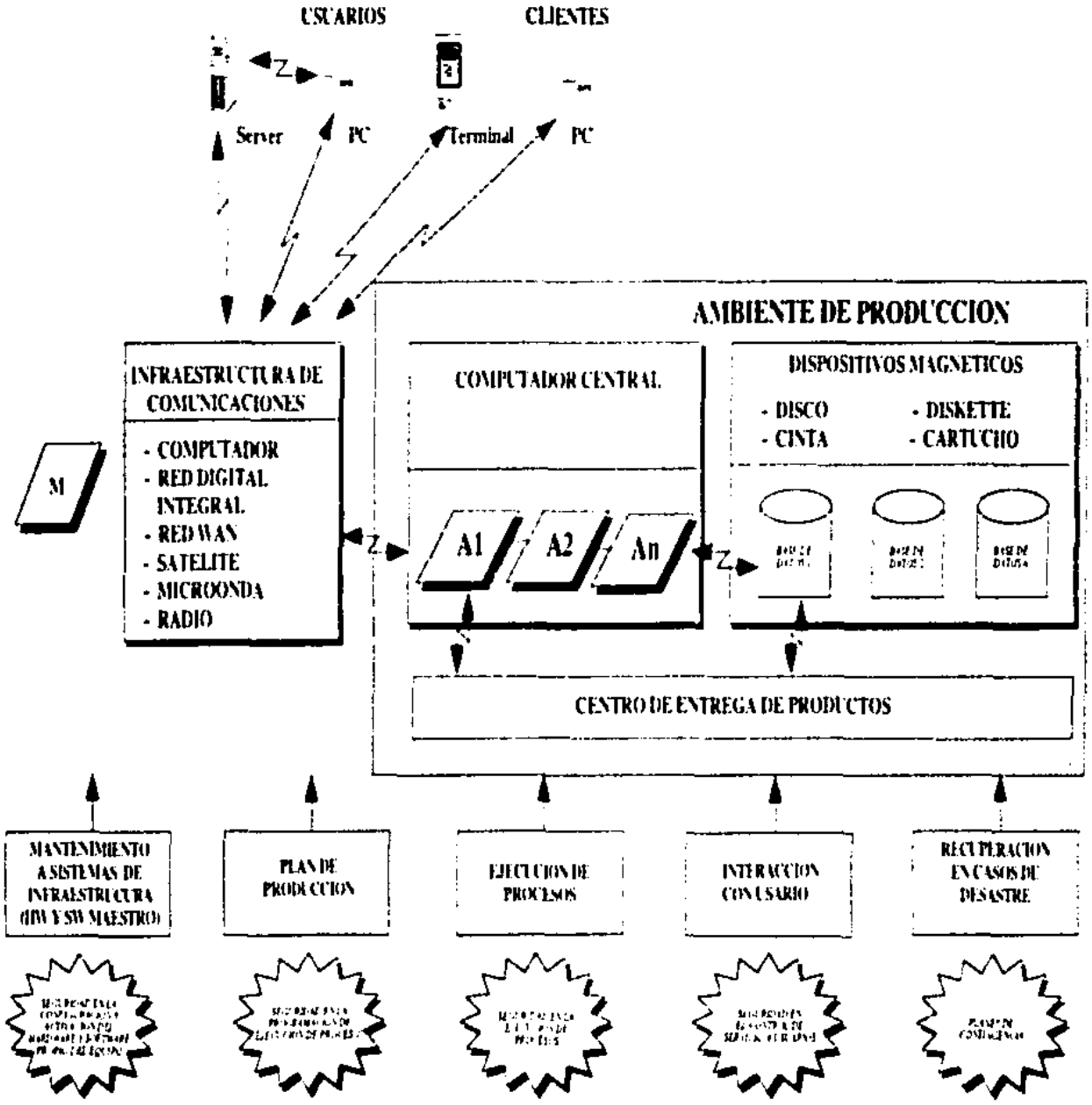
En la etapa de *mantenimiento a sistemas de infraestructura*, se deberá incluir seguridad en la configuración y activación del hardware y software propio del equipo en donde se determinaran las medidas de protección para la configuración el medio ambiente, un esquema de control que permita limitar los comandos de alto riesgo del software de infraestructura así como controles para la actualización de versiones del software propio del equipo de cómputo como son utilerías, sistema operativo, software de seguridad, etc.

Se deberán diseñar también los controles para las bases de datos en donde reside la configuración de los parámetros de seguridad del equipo, establecer reglas de uso y distribución de copias de software,y para el acatamiento de licencias.

En la parte de la elaboración del *plan de producción* se deberá incluir seguridad en la ejecución de procesos en la cual se determinarán los criterios y normas de seguridad para realizar reprocesos, monitoreo y seguimiento de fallas; se deberá certificar durante el establecimiento de los controles que se cumpla con la norma definida así como la implantación de los controles correspondientes.

SEGURIDAD EN MAIN FRAMES

- *Operación*



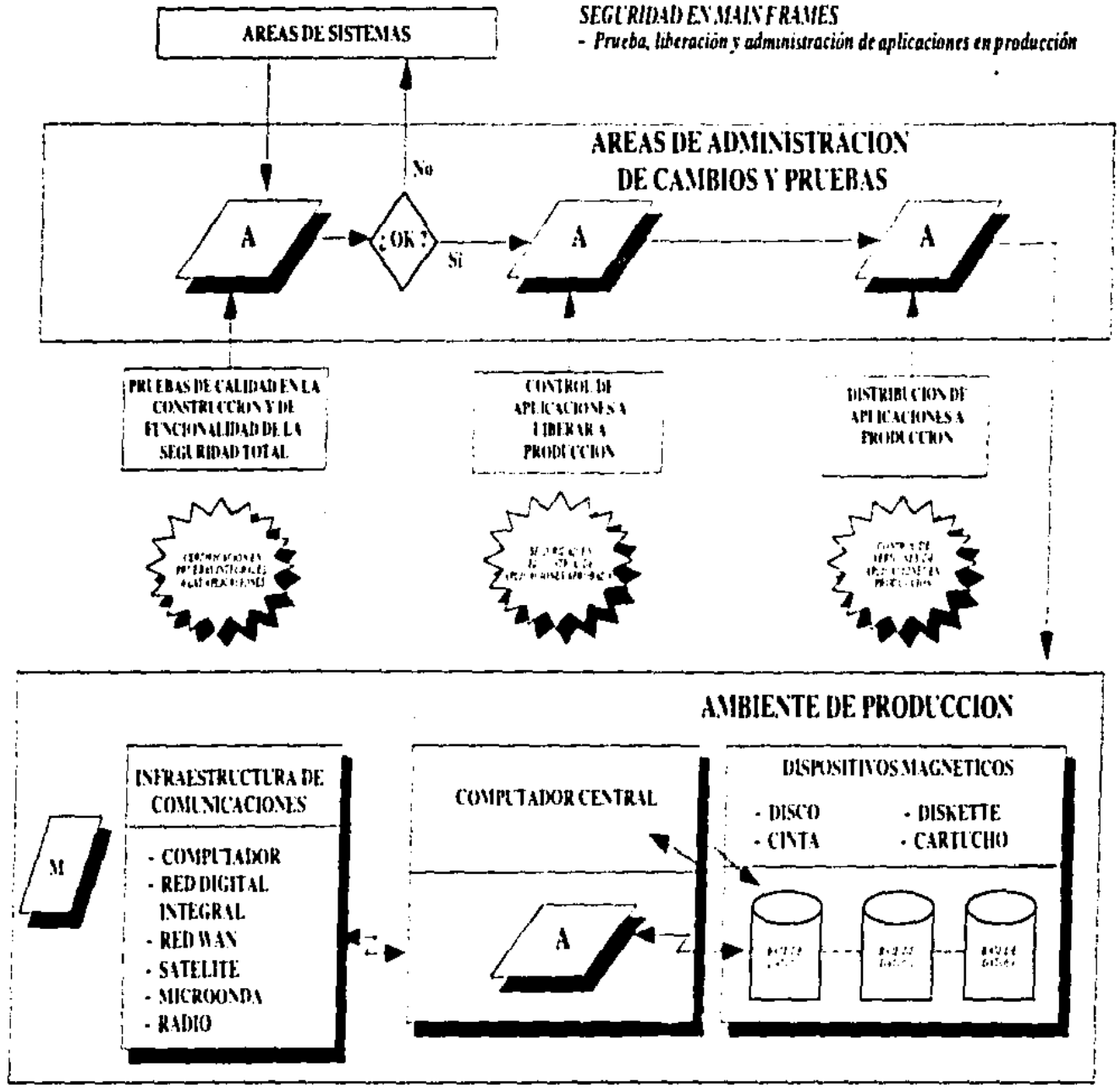
PRUEBA, LIBERACIÓN Y ADMON. DE APLICACIONES EN PRODUCCIÓN

Las *pruebas de calidad en la construcción y de funcionalidad de la seguridad total* a cargo de las áreas de sistemas, deberán incorporar la certificación en pruebas integrales a las aplicaciones las cuales deberán certificar la validez y funcionamiento de las pistas de auditoria para el monitoreo de la aplicación en cuanto a fallas y errores, deberá también incorporar las técnicas que garanticen la confidencialidad, integridad, oportunidad y auditabilidad de la aplicación a liberar en producción y seleccionaran e implantaran medidas de seguridad para la protección de herramientas y recursos de prueba.

La parte del *control de aplicaciones a liberar a producción* a cargo de la función de administración de cambios y pruebas, deberá incluir seguridad en el control de aplicaciones aprobadas y que a su vez deberá de incorporar medidas de seguridad en el control de acceso al código ejecutable para evitar el uso de código no autorizado, establecimiento de medidas de seguridad para garantizar la correspondencia entre código fuente y ejecutable y deberá también determinar las medidas de seguridad para evitar el uso de utilerías de alto riesgo utilizadas en la prueba de programas en el ambiente de producción.

Otra función de la administración de cambios y pruebas es la *distribución de aplicaciones a producción*, la cual deberá incluir el control de versiones en aplicaciones en producción y que deberá contener criterios, políticas y medidas de seguridad para asegurar el uso de versiones validas en producción, el control del acceso y almacenamiento del código objeto de las aplicaciones y el control y registro de las actualizaciones de versiones.

Además deberán dictarse las medidas y mecanismos para activar el uso de versiones de respaldo en caso de necesidad así como certificar que la actualización del software se realiza de manera centralizada a través de sistemas de distribución automatizados.


AREAS DE SISTEMAS
SEGURIDAD EN MAIN FRAMES
- Prueba, liberación y administración de aplicaciones en producción
AREAS DE ADMINISTRACION
DE CAMBIOS Y PRUEBAS
A
¿ OK ?
No
Si
A
A
PRUEBAS DE CALIDAD EN LA CONSTRUCCION Y DE FUNCIONALIDAD DE LA SEGURIDAD TOTAL
CONTROL DE APLICACIONES A LIBERAR A PRODUCCION
DISTRIBUCION DE APLICACIONES A PRODUCCION
AMBIENTE DE PRODUCCION
M
INFRAESTRUCTURA DE COMUNICACIONES
- COMPUTADOR
- RED DIGITAL INTEGRAL
- RED WAN
- SATELITE
- MICROONDA
- RADIO
COMPUTADOR CENTRAL
A
DISPOSITIVOS MAGNETICOS
- DISCO
- DISKETTE
- CINTA
- CARTUCHO

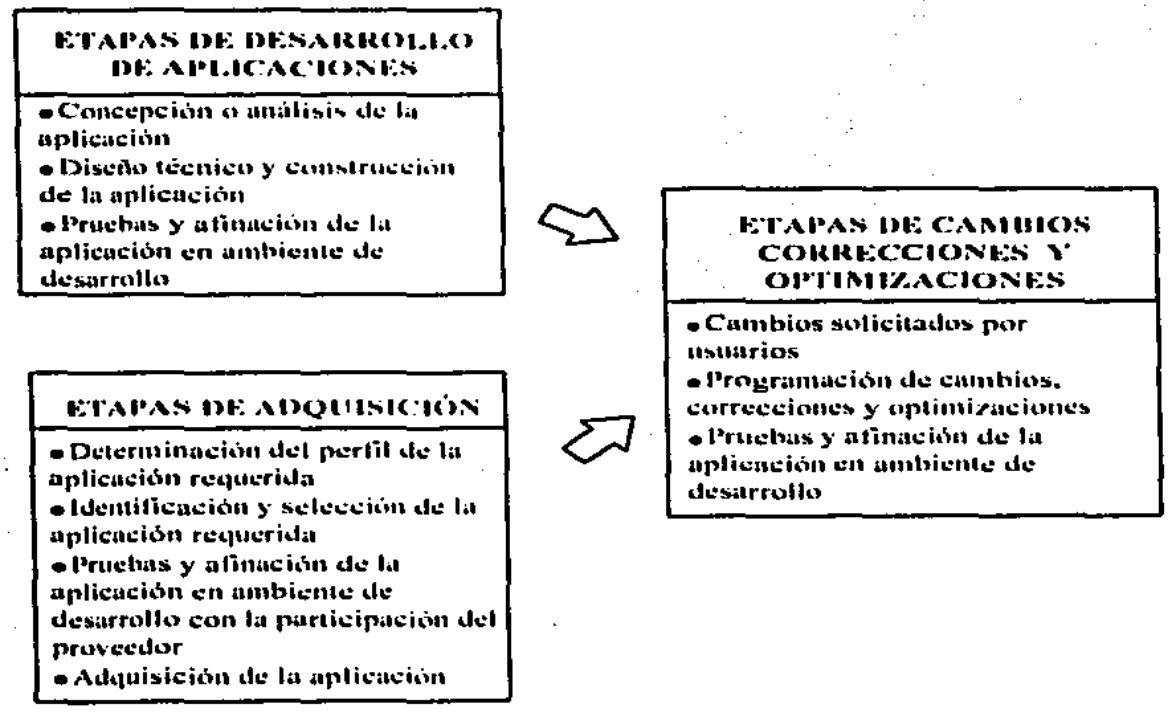
SEGURIDAD EN REDES LOCALES, PC'S Y AMBIENTE CLIENTE SERVIDOR

PROPÓSITO:

Proporcionar los mecanismos de protección en la custodia, procesamiento y distribución de información a través de tecnología cliente-servidor, redes locales y PC's.

RESPONSABILIDADES DEL PROCESO:

- **Establecer mecanismos para la seguridad en el desarrollo, adquisición, administración y configuración de software y aplicaciones para redes locales distribuidas.**
- **Instrumentar el Control de acceso y facultades en redes locales.**
- **Establecer Seguridad en la administración de redes locales.**
- **Definir e implantar protección contra software nocivo.**
- **Definir e implantar protección física en la operación de redes locales y estaciones de trabajo.**
- **Establecer funciones de monitoreo, auditoria y revisiones de seguridad en la operación de redes locales.**
- **Definir, implantar y probar los Planes de contingencia en redes locales.**



ETAPAS DE ACCESO	ETAPAS DE OPERACIÓN	ETAPA DE PRUEBA, LIBERACIÓN Y ADMON. DE APLS. EN PRODUCCIÓN
Acceso local o remoto vía redes (usuarios)	Mantenimiento a redes locales (Hardware y Software maestro)	Pruebas de calidad en la construcción y de funcionalidad total
Acceso Remoto vía redes no autorizadas	Procedimientos para evitar carga de software nocivo	Control de aplicaciones a liberar a producción
Acceso local vía utilerías de operación (Administradores de la red)	Administración de redes locales	Liberación de aplicaciones a producción
	Recuperación en casos de desastre	

- ETAPAS DE DESARROLLO DE APLICACIONES

Los elementos y mecanismos que se deberán considerar en la parte del desarrollo de aplicaciones para ambientes de PC, redes locales y ***cliente servidor*** deberán estar consideradas en las siguientes etapas:

En la etapa del *análisis o concepción de la aplicación* se recomienda implementar parte de la seguridad en datos dentro de la cual se deberán definir los mecanismos de validación de datos, las vistas de acceso a los datos a los usuarios facultados, los tipos de datos que no podrán ser eliminados por los niveles de usuarios privilegiados así como los esquemas y mecanismos de protección a los archivos de datos y bases de datos.

También es recomendable definir la seguridad en el diseño de acceso y facultades para redes locales, esto es, establecer los criterios para determinar las áreas y usuarios que tendrán el derecho a accesar la información, también aquellos criterios que sirvan para identificar las transacciones a utilizar por los usuarios y realizar el analisis de datos sensitivos para establecer los procedimientos de re-autentificacion de transacciones sensitivas.

En esta etapa se deberá considerar lo que corresponde al diseño de seguridad en la información, en donde se determinaran los mecanismos de proteccion y control en los dispositivos magneticos e información impresa así como clasificar la información para su acceso y uso en estos medios, también es importante definir los procedimientos de distribución, custodia y destrucción de aquella información generada en cintas, cartuchos, impresiones, etc. Se recomienda definir estándares de etiquetados de los destinatarios autorizados de la información.

En la segunda etapa *Diseño técnico y construcción de la aplicación*, se tomaran dos elementos de seguridad, el primero es la seguridad en el diseño técnico y programación de aplicaciones en redes locales la cual deberá contener la programación de los algoritmos de seguridad y validación detectados en el análisis tanto para las entradas, salidas, procesos y consultas; se deberán también desarrollar los puntos de reinicio en caso

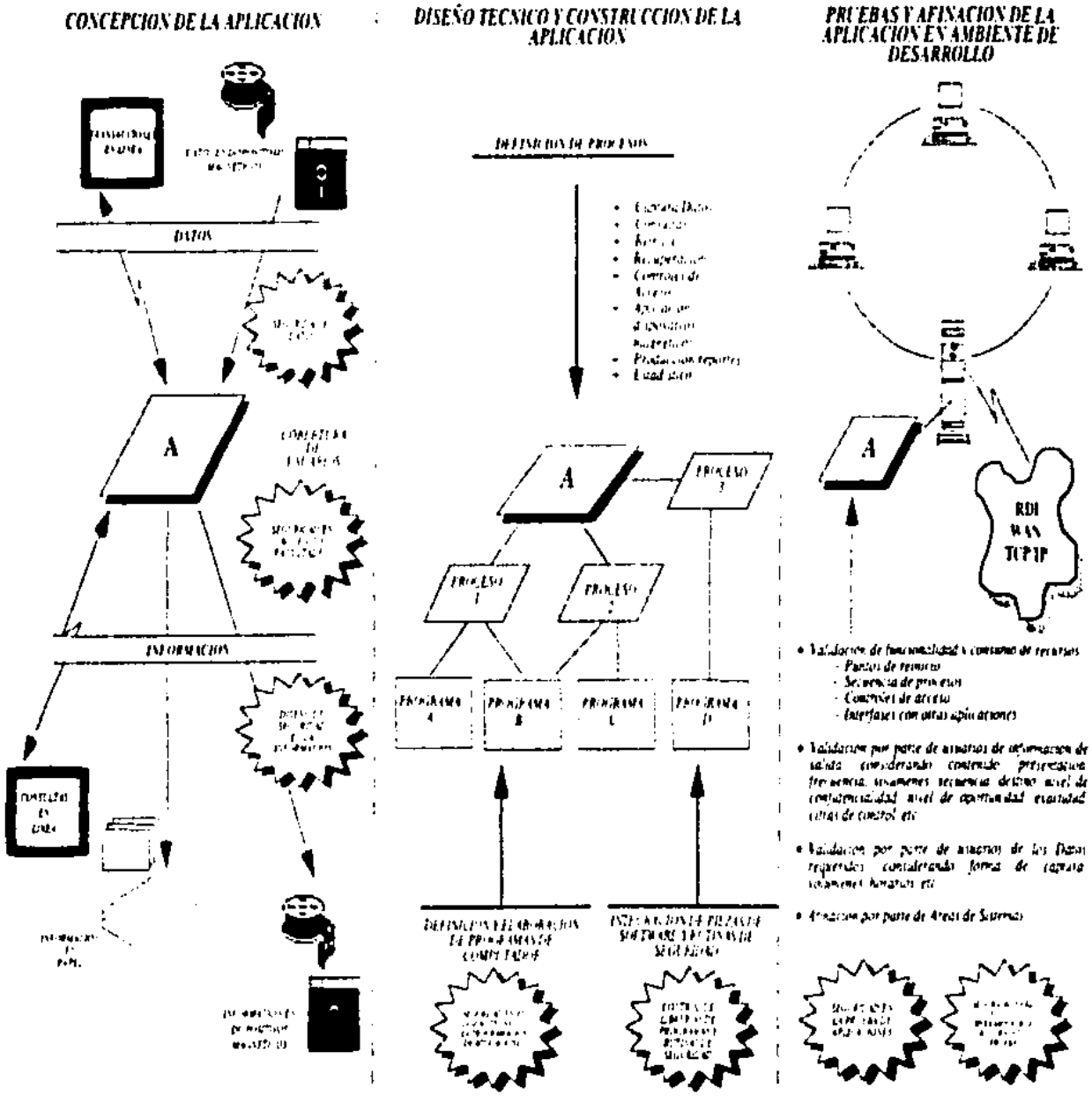
de fallas por SW y HW y programar o activar los registros para las pistas de auditoria. Es importante determinar los tipos de pruebas de escritorio para asegurar que los procesos ofrecen integridad en el manejo de los datos e información.

El segundo elemento de esta etapa es el control de librerías de programas y rutinas de seguridad en redes locales en donde se deberán seleccionar las rutinas o librerías de seguridad que ofrece el proveedor de equipo o software y en caso de ser necesario, desarrollar las interfases que correspondan. Se deberá mantener un control de estas rutinas y librerías definiendo medidas de protección y distribución de copias de estas piezas de software.

La tercera etapa para el desarrollo de aplicaciones en redes locales son las *pruebas y afinación de la aplicación en ambiente de desarrollo* en donde se debe considerar la seguridad en pruebas que incluye la determinación de las reglas de seguridad en el proceso de pruebas como son datos prueba, funcionalidad total, pruebas de escritorio, etc.; se deberán establecer los criterios para documentar el desarrollo y resultados de las pruebas así como su certificación y por último los procedimientos para generar y recuperar las pistas de auditoria.

La siguiente figura esquematiza las etapas y los puntos de seguridad antes descritos.

SEGURIDAD EN REDES LOCALES
- *Desarrollo de Aplicaciones*



ETAPAS DE ADQUISICIÓN DE APLICACIONES

Los puntos y elementos de seguridad que se deberán considerar en la parte de adquisición de aplicaciones para redes locales, PC's, y ambiente *cliente servidor* deberán estar consideradas en las siguientes etapas:

La primera etapa en donde se identifican las necesidades de un desarrollo externo, se toma en cuenta el presupuesto, se analizan a los proveedores y sus condiciones de soporte así como la definición del ambiente en donde deberá correr la aplicación, no se contempla algún punto de seguridad; este se sugiere sea hasta la segunda etapa de *Identificación y selección de la aplicación requerida* en donde deberán existir dos elementos de seguridad, el primero es la seguridad en el diseño técnico y programación de aplicaciones en redes locales la cual deberá contener la programación de los algoritmos de seguridad y validacion detectados en al análisis tanto para las entradas, salidas, procesos y consultas; se deberán también desarrollar los puntos de reinicio en caso de fallas por SW y HW y programar o activar los registros para las pistas de auditoria. Es importante determinar los tipos de pruebas de escritorio para asegurar que los procesos ofrecen integridad en el manejo de los datos e información.

El segundo elemento de esta etapa es el control de librerías de programas y rutinas de seguridad en redes locales en donde se deberán seleccionar las rutinas o librerías de seguridad que ofrece el proveedor de equipo o software y en caso de ser necesario, desarrollar las interfases que correspondan. Se deberá mantener un control de estas rutinas y librerías definiendo medidas de protección y distribución de copias de estas piezas de software.

La tercera etapa para la adquisición de aplicaciones en redes locales son las *pruebas y afinación de la aplicación en ambiente de desarrollo con la participación del proveedor* en donde se debe considerar la seguridad en pruebas que incluye la determinación de las reglas de seguridad en el proceso de pruebas como son datos prueba, funcionalidad total, pruebas de escritorio, etc.; se deberán establecer los criterios para documentar el desarrollo y resultados de las pruebas así como su certificación y por ultimo los procedimientos para generar y recuperar las pistas de auditoria.

En esta etapa se debe considerar la seguridad en el uso de herramientas y recursos de prueba en redes locales en donde debe incluir las medidas para separar el ambiente de prueba del ambiente de producción, aquellas medidas para proteger la confidencialidad de los datos utilizados para fines de las pruebas, seleccionar y en su caso coordinar la implantación de medidas de seguridad para la protección de herramientas y recursos de prueba. Se deberán incluir esquemas de control de versiones y finalmente las medidas para proteger la emisión no autorizada de copias de las aplicaciones propietarias.

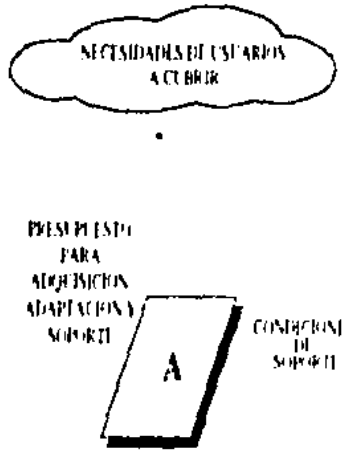
La ultima etapa *Adquisición de la aplicación* deberá contener Seguridad en los convenios con terceros que incluyen los criterios para que las nuevas adquisiciones cumplan con las cláusulas de confidencialidad, derechos patrimoniales, cláusulas de propiedad y medidas de seguridad internas; también se deberán determinar los procedimientos para certificar que las nuevas adquisiciones cumplan con las normas y reglamentos de seguridad para el desarrollo y mantenimiento de la aplicación.

La siguiente figura ejemplifica lo anterior:

SEGURIDAD EN REDES LOCALES

- Adquisición de Aplicaciones

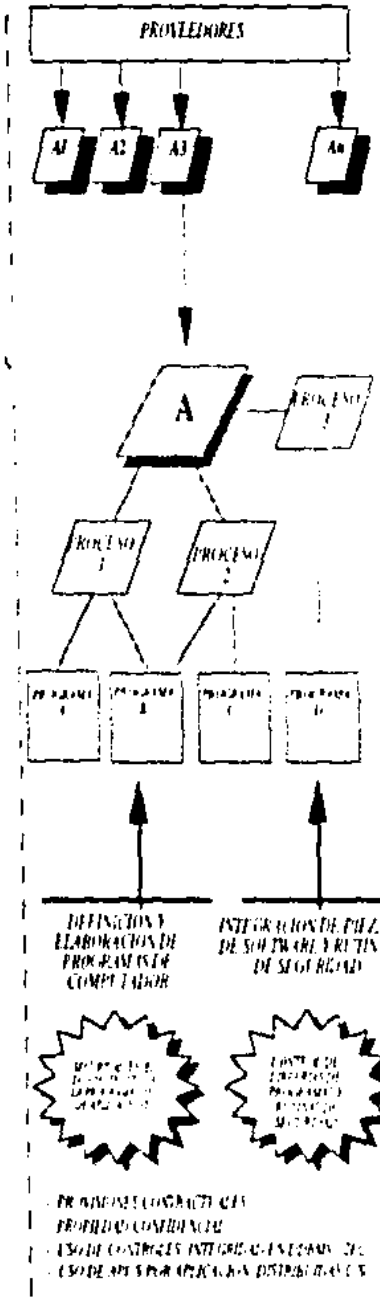
DETERMINACION DEL PERFIL DE LA APLICACION REQUERIDA



AMBIENTE DE PRODUCCION EN QUE CORRERA

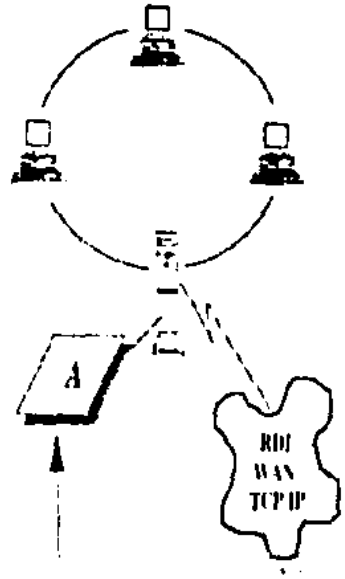
- RED LOCAL DEPARTAMENTAL (NOVELL, UNIX)
- INTERFASE CON MAINFRAME
- OS/2
- WNT
- LAN MGR

IDENTIFICACION Y SELECCION DE LA APLICACION REQUERIDA



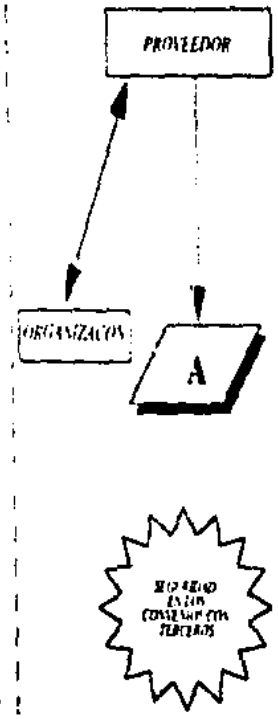
- PROBLEMAS DE COMPATIBILIDAD
- PROBLEMAS DE CONFIABILIDAD
- USO DE CONTROLES INTEGRADOS EN EL SISTEMA OPERATIVO
- USO DE APLICACIONES DISTRIBUIDAS

PRUEBAS Y AFINACION DE LA APLICACION EN AMBIENTE DE DESARROLLO CON PARTICIPACION DEL PROVEEDOR



- *Validacion de funcionalidad y consumo de recursos*
  - *Puntos de reinicio*
  - *Secuencia de procesos*
  - *Controles de acceso*
  - *Interfases con otras aplicaciones*
- *Validacion por parte de usuarios de información de salida, considerando contenido, presentacion, frecuencia, volumenes, secuencia, destino, nivel de confidencialidad nivel de oportunidad, exactitud, cifras de control, etc.*
- *Validacion por parte de usuarios de los Datos requeridos, considerando forma de captura, volumenes, horarios, etc*
- *Afinacion por parte Area de Sistemas*

ADQUISICION DE LA APLICACION



ETAPAS DE CAMBIOS, CORRECCIONES Y OPTIMIZACIONES

Los elementos de seguridad que se deberán considerar en la parte de cambios, correcciones y optimizaciones de aplicaciones para redes locales, PC's, y ambiente ***cliente servidor*** deberán estar consideradas en las siguientes etapas:

En la etapa de cambios se debe considerar la seguridad en el uso de herramientas y recursos de prueba en redes locales en donde debe incluir las medidas para separar el ambiente de prueba del ambiente de producción, aquellas medidas para proteger la confidencialidad de los datos utilizados para fines de las pruebas, seleccionar y en su caso coordinar la implantación de medidas de seguridad para la protección de herramientas y recursos de prueba. Se deberán incluir esquemas de control de versiones y finalmente las medidas para proteger la emisión no autorizada de copias de las aplicaciones propietarias.

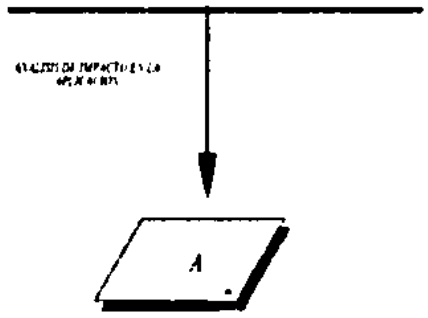
También se debe incluir seguridad en cambios o adición a la aplicación en donde se deberán especificar los criterios para incorporar puntos de control de seguridad en los cambios realizados, asegurar el uso de controles para registrar todos los cambios realizados y aquellos controles para verificar la consistencia del código fuente con su código objeto, determinar los controles de acceso y pistas de auditoria para proteger los archivos y las librerías de programas.

La seguridad en el diseño técnico y programación de aplicaciones en redes locales, el control de librerías de programas y rutinas de seguridad en redes locales, la seguridad en pruebas y la seguridad en el uso de herramientas y recursos de prueba que se han definido anteriormente deberán ser elementos a considerar en las etapas que se expresan gráficamente en la figura siguiente:

SEGURIDAD EN REDES LOCALES
- Cambios, correcciones y optimizaciones

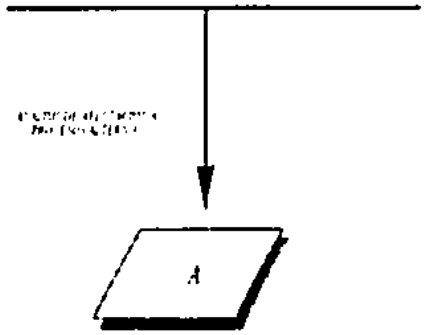
CAMBIOS SOLICITADOS POR USUARIOS

USUARIOS



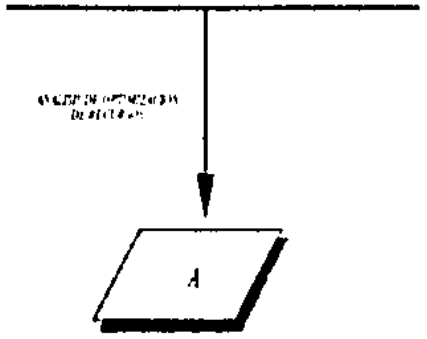
CORRECCIONES POR FALLAS EN PRODUCCION

ADMINISTRADOR DE LA RED Y USUARIOS



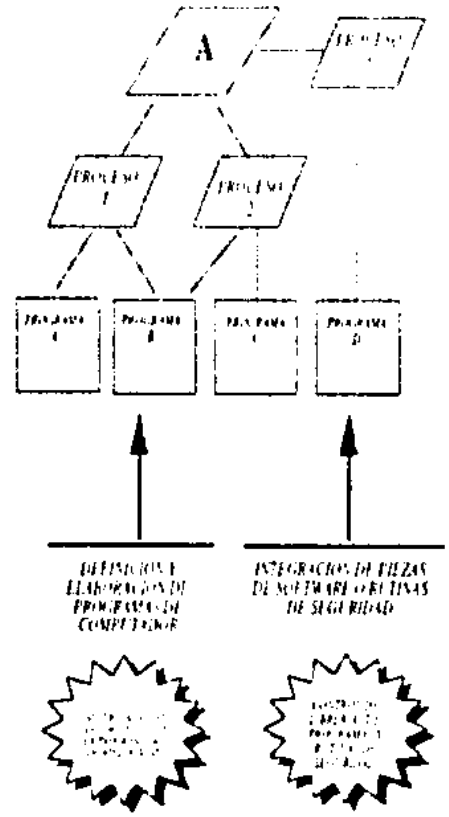
OPTIMIZACIONES A LA APLICACION EN EL USO DE LOS RECURSOS DE COMPUTO

INGENIERIA DE SISTEMAS



PROGRAMACION DE CAMBIOS, CORRECCIONES Y OPTIMIZACIONES

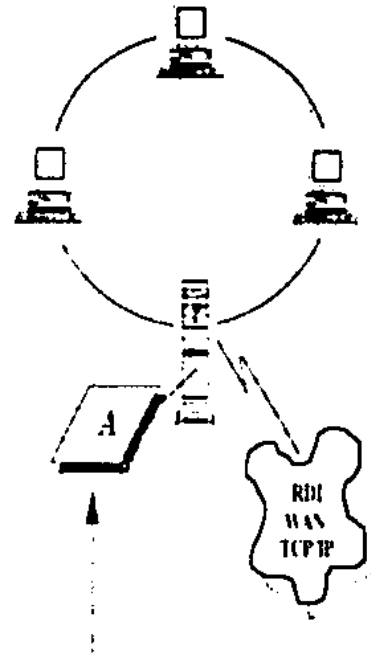
INTEGRACION DE CAMBIOS CORRECCIONES Y OPTIMIZACIONES EN LOS PROCESOS Y EN LOS PROGRAMAS



DEFINICION Y ELABORACION DE PROGRAMAS DE COMPUTADOR

INTEGRACION DE PIEZAS DE SOFTWARE O RUTINAS DE SEGURIDAD

PRUEBAS Y AFINACION DE LA APLICACION EN AMBIENTE DE DESARROLLO



- *Validacion de funcionalidad y consumo de recursos*
  - *Puntos de retardo*
  - *Secuencia de procesos*
  - *Controles de acceso*
  - *Interfases con otras aplicaciones*
- *Validacion por parte de usuarios de información de salida, considerando contenido, presentacion, frecuencia volumenes, secuencia, destino, nivel de confidencialidad, nivel de oportunidad, exactitud, cifras de control, etc.*
- *Validacion por parte de usuarios de los Datos requeridos, considerando forma de captura, volumenes, horarios, etc*
- *Afinacion por parte Areas de Sistemas*

ETAPAS DE ACCESO Y OPERACIÓN

Dentro de la parte de acceso y operación se deberán considerar cinco aspectos para contribuir a que la seguridad sea incrementada. Las tres etapas de acceso local o remoto vía redes para usuarios de aplicaciones, el acceso remoto vía otras redes (aquellos que posean Internet, o redes WAN) y el acceso local vía utilerías de operación (administradores de seguridad); deberán ser verificados por el Control de Acceso y Facultades en redes Locales cuyos principales objetivos son los de implantar un modelo se seguridad acorde a las características de conexión estableciendo controles confiables de identificación y autentificación de usuarios definiendo claramente los niveles de facultades tanto en aplicaciones como en el software de infraestructura.

La etapa de mantenimiento a Redes Locales tanto en software como hardware maestro, deberá contener dentro de la Configuración y Activación del Hardware y Software propio del equipo, las medidas de protección en la configuración del medio ambiente, un esquema de control que deberán tener los comandos y control de versiones del software de infraestructura, se deberán determinar también los controles que deberán aplicarse a las bases de datos donde reside la configuración de seguridad del equipo (como direcciones de enlaces, claves de acceso, etc.).

La etapa de operación de procedimientos que evitan la carga en la red local de software nocivo deberán ser consideradas las medidas para la identificación y control de software nocivo, la validación de estrategias para la prevención y combate de dicho software, control de nuevas versiones y actualizaciones y definir procedimientos para reportar incidentes y corregir las "infecciones".

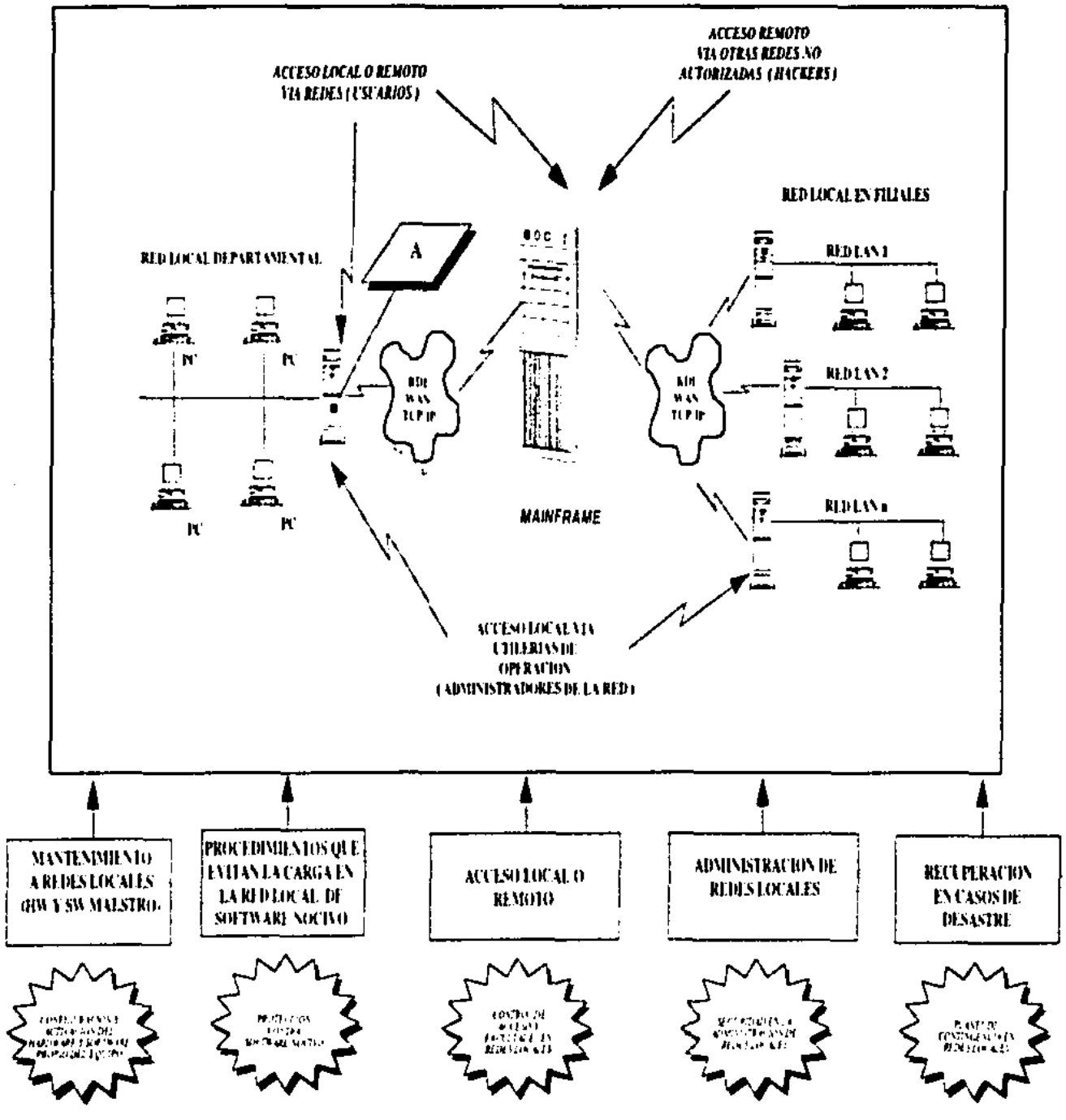
En etapa de la Seguridad en la Administración de redes Locales es recomendable determinar las medidas de seguridad en los recursos de cómputo y medios magnéticos removibles en cuanto a su asignación, custodia, uso y distribución. También se deberá incluir la medidas para las redes privilegiadas así como el monitoreo en el cumplimento de las políticas de uso de redes locales.

El plan maestro de contingencias para redes locales, la identificación de procesos críticos en las mismas, la certificación de la implantación y prueba de las planes de contingencia y la determinación de las estrategias y procedimientos de respaldo de datos y protección fuera del site (centro de cómputo); son funciones y actividades que deberá contener la etapa de Planes de Contingencia en redes Locales.

La siguiente figura esquematiza los puntos de seguridad que deberán ser incluidos en el acceso y operación de las redes locales:

SEGURIDAD EN REDES LOCALES Y PC'S

- *Acceso y Operación*



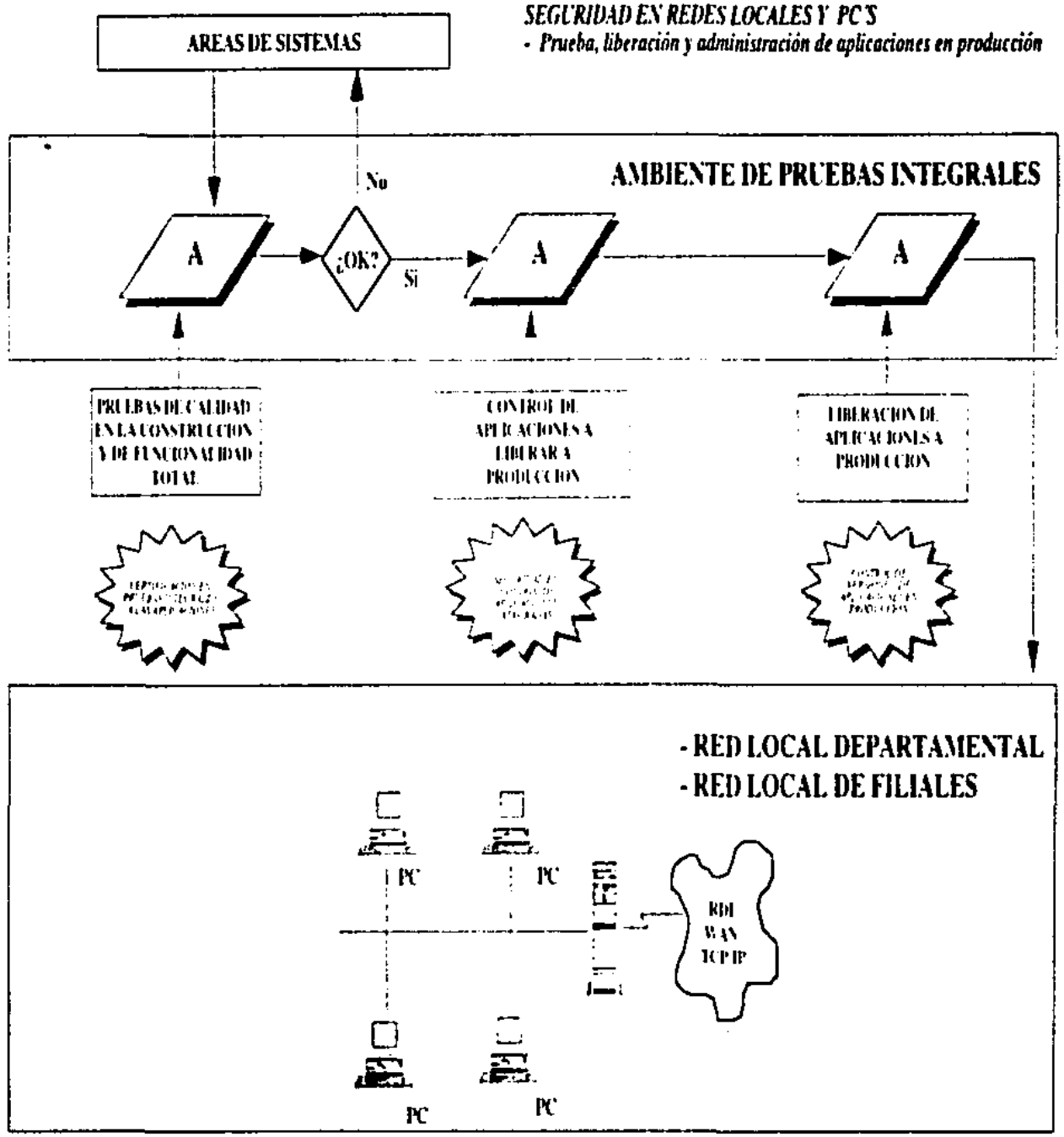
PRUEBA, LIBERACIÓN Y ADMON. DE APLICACIONES EN PRODUCCIÓN

Las *pruebas de calidad en la construcción y de funcionalidad de la seguridad total* a cargo de las áreas de sistemas, deberán incorporar la certificación en pruebas integrales a las aplicaciones las cuales deberán certificar la validez y funcionamiento de las pistas de auditoria para el monitoreo de la aplicación en cuanto a fallas y errores, deberá también incorporar las técnicas que garanticen la confidencialidad, integridad, oportunidad y auditabilidad de la aplicación a liberar en producción y seleccionaran e implantaran medidas de seguridad para la protección de herramientas y recursos de prueba.

La parte del *control de aplicaciones a liberar a producción* a cargo de la función de administración de cambios y pruebas, deberá incluir seguridad en el control de aplicaciones aprobadas y que a su vez deberá de incorporar medidas de seguridad en el control de acceso al código ejecutable para evitar el uso de código no autorizado, establecimiento de medidas de seguridad para garantizar la correspondencia entre código fuente y ejecutable y deberá también determinar las medidas de seguridad para evitar el uso de utilerías de alto riesgo utilizadas en la prueba de programas en el ambiente de producción.

Otra función de la administración de cambios y pruebas es la *distribución de aplicaciones a producción*, la cual deberá incluir el control de versiones en aplicaciones en producción y que deberá contener criterios, políticas y medidas de seguridad para asegurar el uso de versiones validas en producción, el control del acceso y almacenamiento del código objeto de las aplicaciones y el control y registro de las actualizaciones de versiones.

Además deberán dictarse las medidas y mecanismos para activar el uso de versiones de respaldo en caso de necesidad así como certificar que la actualización del software se realiza de manera centralizada a través de sistemas de distribución automatizados.


SEGURIDAD EN REDES LOCALES Y PC'S
- Prueba, liberación y administración de aplicaciones en producción
AREAS DE SISTEMAS
AMBIENTE DE PRUEBAS INTEGRALES
No
A
¿OK?
Si
A
A
PRUEBAS DE CALIDAD EN LA CONSTRUCCION Y DE FUNCIONALIDAD TOTAL
CONTROL DE APLICACIONES A LIBERAR A PRODUCCION
LIBERACION DE APLICACIONES A PRODUCCION
- RED LOCAL DEPARTAMENTAL
- RED LOCAL DE FILIALES
PC
PC
PC
PC
RDI
WAN
TCP IP

SEGURIDAD EN COMUNICACIONES

PROPÓSITO:

Implantar medidas de seguridad en los dispositivos de hardware, herramientas de software y mensajes enviados a través de la red de comunicaciones.

RESPONSABILIDADES:

- Seguridad en la configuración y parametrización del software de teleproceso y comunicaciones.
- Seguridad en la administración y operación del servicio de teleproceso y comunicaciones.
- Encripción de información sensitiva que viaje a través de la red de teleproceso.

El módulo o etapa de Seguridad en nuevos sistemas y productos de comunicaciones deberá contener la reglamentación de los controles de acceso lógico para proteger los dispositivos programables de comunicaciones , los mecanismos de autentificación e integridad en los nuevos productos de comunicaciones desarrollados, y en esta etapa también se deberán determinar las medidas de seguridad de eventos y monitoreo a contemplar por los sistemas y productos de comunicaciones.

La Seguridad en la administración, configuración y activación del software de comunicaciones deberá contemplar las medidas de seguridad que deberán considerarse al configurar el software de comunicaciones, debará contener un esquema de control para el uso restringido de los comandos de configuración y uso del software de comunicaciones así como los procedimientos para contar con controles de cambios de software y su documentación. Se deberan también determinar las medidas de seguridad para acotar la cobertura de acceso y administración de la red de comunicaciones, los indicadores de monitoreo y analizar, interpretar y reportar las estadísticas resultantes del monitoreo, en cumplimiento a las medidas, políticas y procedimientos de seguridad establecidos.

Para la etapa de Seguridad en la operación de la red de comunicaciones se deberán determinar:

Estrategias de encripción a usarse en la red de comunicaciones.

Mecanismos y procedimientos para la administración de las llaves de encripción.

Medidas de seguridad para los enlaces de comunicaciones con propios y terceros.

Cláusulas de seguridad informática que deberán contemplarse en los contratos de servicio con terceros en materia de comunicaciones.

También se deberá identificar y seleccionar los mejores esquemas de encripción por enlace y servicios a proteger, dar seguimiento a situaciones de excepción y durante la configuración de los productos de

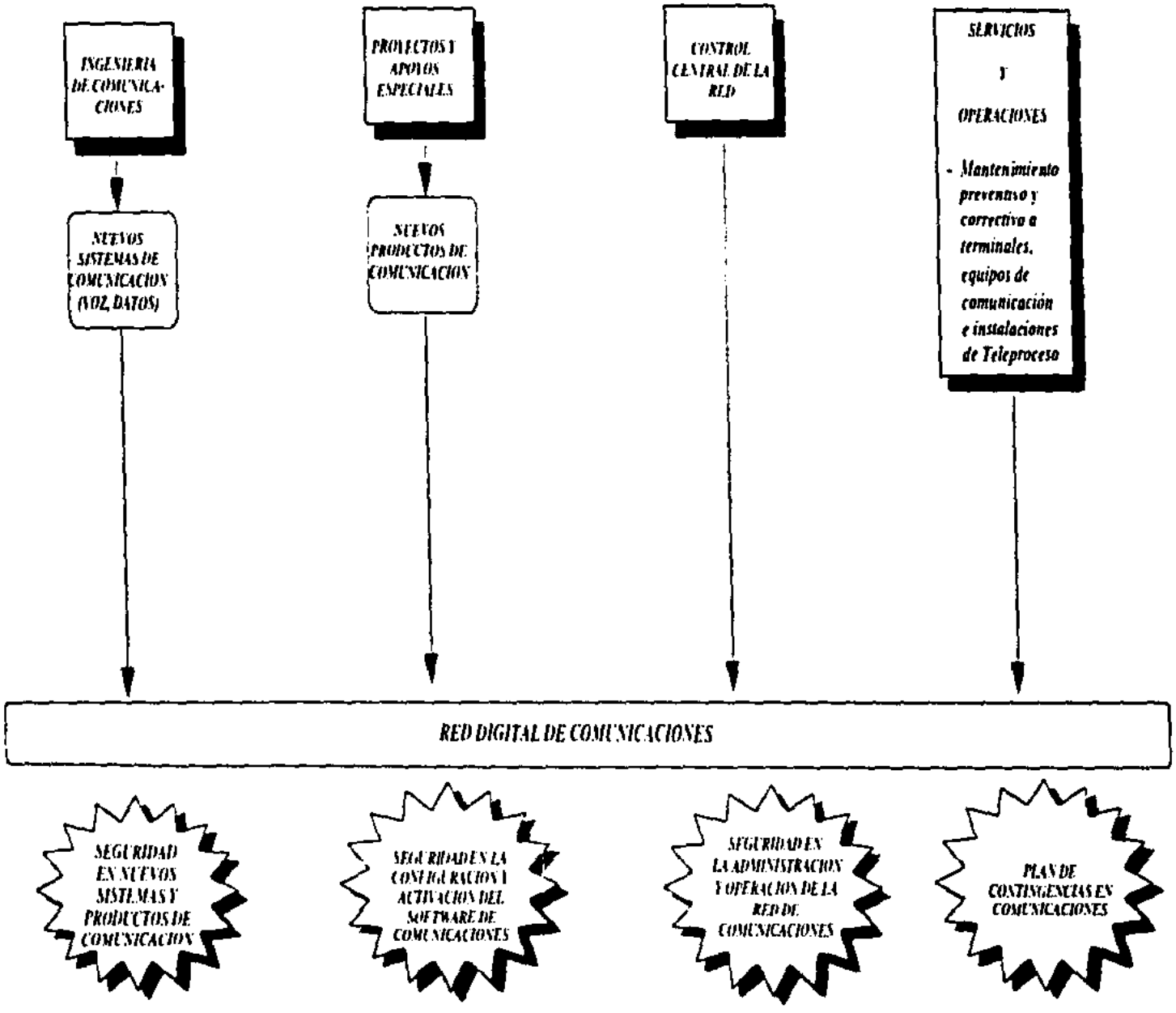
comunicaciones, asegurar que la asignación de los enlaces y usuarios facultados corresponda a la concepción y requerimientos iniciales establecidos.

En la cuarta etapa de Plan de contingencias en comunicaciones se deberán establecer las estrategias del plan maestro de contingencias de comunicaciones, se deberán identificar los nodos, enlaces y procesos críticos a soportar en caso de una contingencia, se deberá apoyar a la implantación del plan maestro de contingencias de comunicaciones.

Es importante establecer un programa de simulacros llevando un control de las pruebas, ajustes y requerimientos y finalmente, certificar la implantación del plan maestro de contingencias de comunicaciones.

La siguiente figura esquematiza lo anterior:

SEGURIDAD EN COMUNICACIONES
- Red Digital



SEGURIDAD EN INFORMACIÓN NO AUTOMATIZADA

PROPÓSITO:

Proteger el uso de la información no automatizada durante sus etapas de registro, transferencia, operación, distribución y custodia.

La Información No Automatizada es la almacenada, representada o involucrada por medios como son cartuchos, medios magnéticos, papel, voz, microfichas, videos, etc.

RESPONSABILIDADES:

- Seguridad en el registro, transferencia, operación y reproducción de información no automatizada.
- Seguridad en la distribución y custodia de la información no automatizada.
- Seguimiento y control del uso de la información.
- Desarrollo de campañas de concientización y capacitación en la materia.

ETAPAS PARA LA PRUEBA, LIBERACIÓN Y ADMINISTRACION DE APLICACIONES EN PRODUCCIÓN	ETAPAS PARA LA SEGURIDAD EN LA REPRODUCCIÓN, CUSTODIA, DISTRIBUCIÓN Y DESTRUCCIÓN DE INFORMACIÓN
Seguridad en la información de entrada a procesos automatizados.	Seguridad en la reproducción, custodia, distribución y destrucción de la información.
Seguridad en la información de salida de procesos automatizados.	

ETAPAS PARA LA PRUEBA, LIBERACIÓN Y ADMINISTRACION DE APLICACIONES EN PRODUCCIÓN

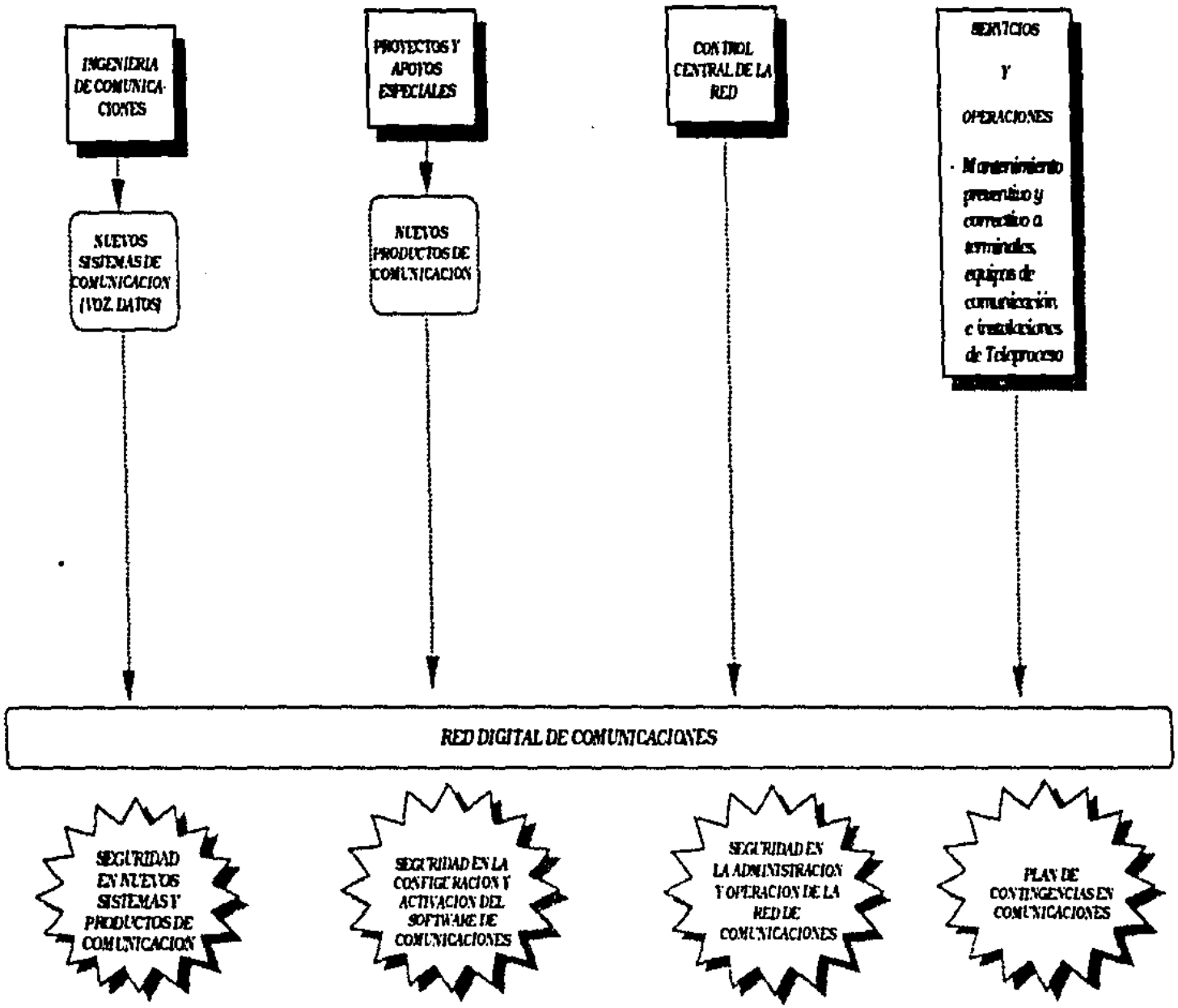
En la primera etapa de Seguridad en la Información de entrada a procesos automatizados se deberán determinar los controles para la recepción de información, aquellos para certificar que la información recibida por los usuarios sea completa, veraz y exacta, así como los controles para almacenar, custodiar y destruir la información una vez que se haya introducido a los procesos automatizados. También se deberán definir políticas y procedimientos para restringir el acceso a la información en papel y dispositivos magnéticos únicamente al personal facultado.

La determinación de controles para la distribucion de información, políticas y procedimientos de destrucción de información no requerida, controles de verificación para asegurar la integridad de la información obtenida de procesos automatizados y el seguimiento a situaciones de excepción; son elementos que se deberán

considerar y definir en la segunda etapa de Seguridad en la Información de salida de los procesos automatizados.

Se explica gráficamente en el diagrama siguiente:

SEGURIDAD EN COMUNICACIONES
- Red Digital

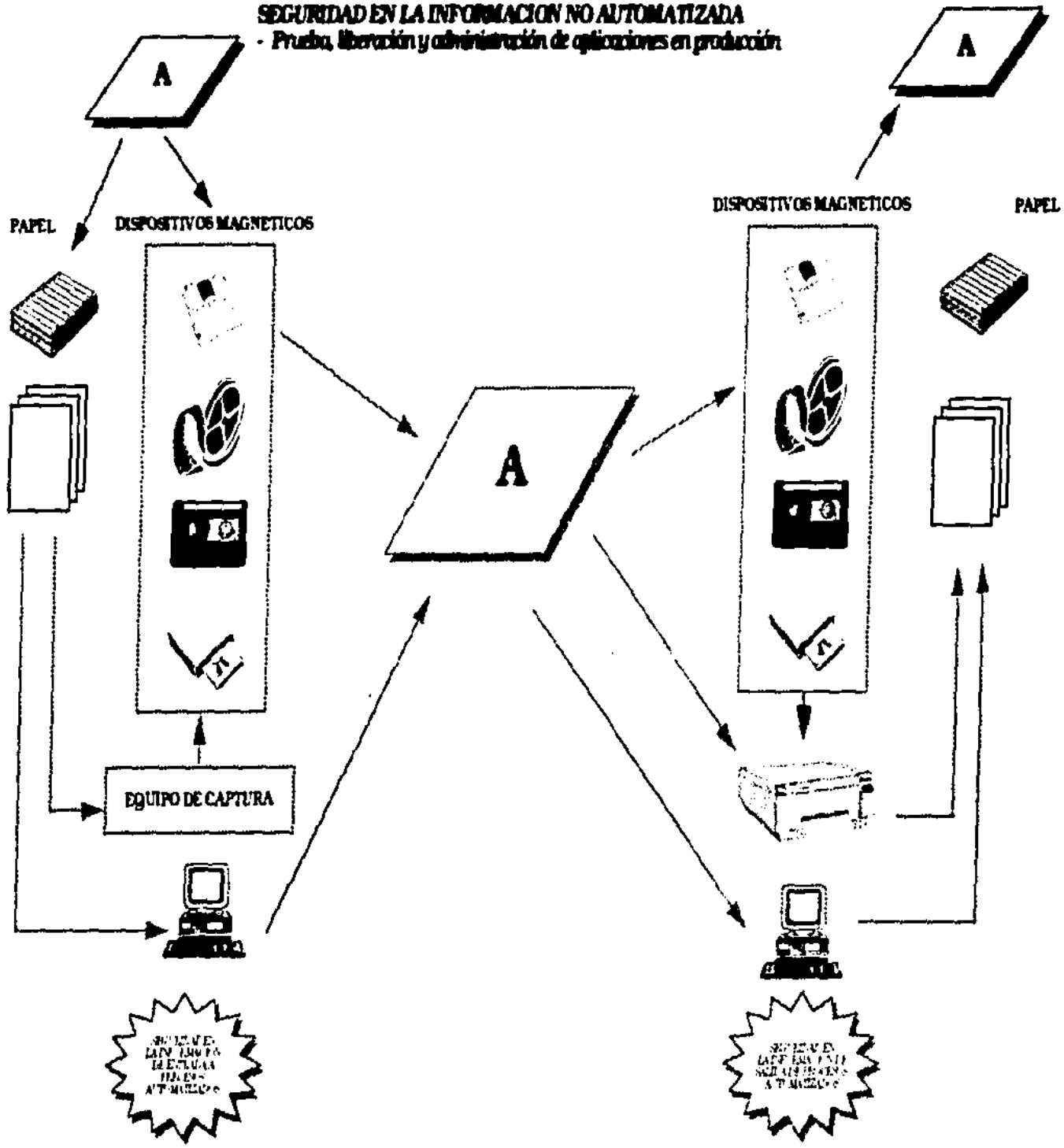


ETAPAS PARA LA SEGURIDAD EN LA REPRODUCCIÓN, CUSTODIA, DISTRIBUCIÓN Y DESTRUCCIÓN DE INFORMACIÓN

La etapa de Seguridad en la reproducción, custodia, distribución y destrucción de la información, deberá contener los controles para la identificación de contenidos en dispositivos magnéticos, controles para la distribución y custodia de información de acuerdo al tipo de clasificación de la misma, también se deberá determinar los mecanismos de protección y control en los dispositivos de reproducción de información.
Es necesario determinar los procedimientos y políticas para la destrucción de información de acuerdo al tipo y clasificación de la misma, y aquellos procedimientos para monitorear y determinar la vigencia de las medidas de seguridad establecidas e incluir elementos para el seguimiento a situaciones de excepción en violaciones de seguridad de la información.
Estos controles, políticas y procedimientos deberán aplicar como la figura siguiente lo representa, tanto en las áreas operativas y de apoyo como en las áreas de custodia de información:

SEGURIDAD EN LA INFORMACION NO AUTOMATIZADA

- **Prueba, liberación y administración de aplicaciones en producción**



CAPITULO V

CONTROLES BÁSICOS DE SEGURIDAD

Entre el nivel de acceso y la seguridad se debe establecer un compromiso, es decir, estos dos temas están en una balanza. El sistema más seguro es el que comparte nada, el más vulnerable es aquel que da todo sin saber a quién; así se quiere dar acceso fácil a todo, pero teniendo control sobre todo.

El problema de las computadoras, las redes que las unen y la seguridad de los datos que guardan las computadoras es análogo al problema de los pueblos, las vías de comunicación y las barreras o controles que se establecen para la protección de los pueblos. Si no tenemos carreteras y nadie externo puede llegar al pueblo, es seguro que nadie nos atacará pero esto no nos permitiría el intercambio, que es una gran fuente de ideas y recursos.

Por ello, para establecer una política de seguridad se recomienda construir carreteras y permitir un libre tráfico pero con verificación de los elementos que desean entrar en el pueblo, es decir, no se cierran las carreteras para verificar quién circula, se ponen controles al momento de acceso al pueblo y después dentro del pueblo se ponen controles estrictos en los centros y actividades neurálgicas o vitales para el desarrollo del pueblo.

Es decir, no se trata de asociar un policía a cada visitante, sino de establecer una bitácora en cada punto vital y que constantemente se este analizando para detectar los puntos que están siendo atacados o con grandes posibilidades de que lo sean.

Por ejemplo, en los bancos las bitácoras son las cámaras de filmación, los detectores de movimiento y paso de objetos por medio de rayos infrarrojos en zonas vitales, etc. Es decir, no se impide el acceso al banco a los clientes que quieren hacer operaciones bancarias, sino se supervisan.

Un problema con los aspectos de seguridad es irse a los extremos en su análisis, así, al minimizar los posibles daños o exagerar que todo puede estar bajo amenaza, trae como consecuencia una parálisis o lentitud enorme en el desempeño de las actividades; es decir, resulta más caro el remedio que la enfermedad.

ANÁLISIS DE LAS AMENAZAS Y PELIGROS

La seguridad es una protección de algo contra alguien o algo. Entre las amenazas y peligros más frecuentes se tiene:

- Acceso al sistema por usuarios no autorizados.
- Pérdida del acceso a la información.
- Acceso negado a la información.
- Comportamiento fraudulento de usuarios permitidos.

Todos los peligros y amenazas siempre deben analizarse pensando en el número de usuarios que pueden ser afectados y en la importancia de la información que está en juego; es por esto que surge nuestra pregunta:

¿Es conveniente aislar los centros vitales?

La disyuntiva en la seguridad es: ¿aislar los centros vitales o poner guardianes a la entrada?, cada una de las soluciones tiene sus ventajas e inconvenientes.

El aislar un centro vital del resto del mundo (trabajar con máquinas sin conexión con el exterior) es una solución extrema, esta facilita la seguridad pero impide un funcionamiento adecuado de los servicios. Con una máquina aislada y evitando todo contacto exterior por medio de red o entrada remota, es menos factible tener problemas con la seguridad.

De todos es conocido que la seguridad es una cuestión de práctica, sentido común y flexibilidad para el cambio, una política de seguridad debe instrumentarse rápido, estar en constante revisión y ser acorde al funcionamiento cotidiano de lo que se quiere supervisar. Si quiero supervisar algo que todo es color negro, no se debe tener al supervisor de color blanco, sino también negro. En la tienda de autoservicio el supervisor debe ser igual a un cliente y no tener una característica que lo distinga.

FLEXIBILIDAD PARA EL CAMBIO.

Un gran problema con la seguridad es que se desea una solución que se instrumente una sola vez y se pretende con esta solución "técnicamente perfecta" instalada, nunca más tener problemas; esto no es así generalmente, *la seguridad inicia en algún momento y nunca se termina de instrumentar.*

Todo el tiempo se requieren afinaciones y adecuaciones, ya que los peligros, amenazas y problemas de acceso no autorizado evolucionan. El problema de la intrusión al sistema operativo por los famosos virus y sus vacunas es un buen ejemplo, siempre se requiere actualizar un nueva vacuna. Aquí nos surge la pregunta ¿quién obtiene el mayor beneficio de la existencia de los virus?, es tanto como imaginar que los automóviles no requerirán nunca mantenimiento, ni cambio de refacciones, no sufrirán desgaste, etc., finalmente el hecho de existir una guerra entre vacunas y virus refleja la necesidad de coexistir, si no hubiera virus nadie tendría que invertir en la compra de una vacuna y por lo tanto este mercado no existiría. Se puede llegar a la reflexión que el mismo que desarrolla los virus tiene el antivirus y así incrementar sus ganancias en la venta de estos últimos.

A continuación se presentarán los principios para hacer funcionar, comprobar e inspeccionar el desempeño de los niveles y avances en la seguridad informática; éstos los denominaremos "controles básicos de seguridad" y estarán divididos en:

A) POLÍTICAS DE LA ORGANIZACIÓN
B) SEGURIDAD FÍSICA
C) SEGURIDAD EN COMUNICACIONES
D) SEGURIDAD LÓGICA

A) POLÍTICAS DE LA ORGANIZACIÓN

En esta sección se listan las políticas generales de seguridad que deberán surgir desde los niveles más altos de la organización y las cuales deberán ser las directrices para un programa completo de seguridad informática. El siguiente cuadro muestra los aspectos a considerar para la definición de las políticas de la organización.

POLÍTICAS DE LA ORGANIZACIÓN

- A.1 Políticas y estándares de seguridad.
- A.2 Concientización.
- A.3 Apoyo gerencial.
- A.4 Capacitación.
- A.5 Roles y responsabilidades dentro de la organización.
  - A.5.1 Función de seguridad en la información.
  - A.5.2 Responsabilidad de la información.
  - A.5.3 Administradores y coordinadores de seguridad.
  - A.5.4 Autoridad limitada.
  - A.5.5 Seguridad en la descripción de puestos.
  - A.5.6 Comité de seguridad informática.
  - A.5.7 Auditoría en sistemas.
  - A.5.8 Personal de la función de seguridad informática.
- A.6 Autorizaciones, acuerdos y contratos.
  - A.6.1 Contratos.
  - A.6.2 Autorización de uso.
  - A.6.3 Seguros.
- A.7 Desarrollo y adquisición de sistemas.
  - A.7.1 Responsabilidades en el desarrollo.
  - A.7.2 Ambiente de pruebas.

A continuación se hace un desglose de manera más detallada de las directrices y orientaciones que se deberán contemplar en un programa de seguridad

A.1	POLÍTICAS Y ESTÁNDARES DE SEGURIDAD.
A.1.1	Desarrollar y difundir políticas de Seguridad Informática para toda la organización.
A.1.2	Desarrollar y publicar estándares y lineamientos que soporten las políticas de Seguridad Informática.
A.1.3	Implementar y promover una política de confidencialidad, basada en la "necesidad de conocer" o "necesidad de conservar".
A.1.4	Actualizar y apoyar las políticas, estándares y lineamientos sobre bases regulares y de acuerdo a los cambios principales que ocurran.
A.1.5	Establecer una política de escritorios limpios[5] en áreas que manejan información sensitiva.

[5] Se requiere concientizar al personal en la necesidad de mantener toda la información impresa, en medios magnéticos, videocintas, etc., guardados bajo llave con la finalidad de no exhibir información de alto riesgo y que sea utilizada con afán de dolo por parte de extraños.

A.2	CONCIENTIZACIÓN
A.2.1	Desarrollar e implementar programas de concientización y motivación hacia toda la empresa con información actualizada de seguridad en cómputo y comunicación.
A.2.2	Compartir la responsabilidad de los programas de concientización de seguridad informática con los administradores locales de seguridad
A.2.3	Adoptar un código ético de conducta que incluya la preservación de la propiedad de la información.
A.2.4	Requerir revisiones periódicas y compromiso con el código de ética de todo el personal de la organización.

A.3	APOYO GERENCIAL
A.3.1	Motivar y educar a la alta gerencia sobre Seguridad Informática para poder obtener su reconocimiento, apoyo e interés de la protección de activos informáticos.
A.3.2	Obtener apoyo de todos los niveles gerenciales para el programa de Seguridad Informática.

A.4	CAPACITACIÓN
A.4.1	Desarrollar e implementar un programa de capacitación en Seguridad Informática para todos los empleados internos y empleados que interactúan con los sistemas de información de la organización.
A.4.2	Asegurar que los nuevos empleados asistan a una sesión de capacitación sobre Seguridad Informática.
A.4.3	Presentar sesiones de actualización sobre Seguridad Informática a los gerentes y a todos los empleados.
A.4.4	Coordinar sesiones de capacitación con los tópicos de Seguridad Informática en programas motivacionales.
A.4.5	Capacitar a todo el personal responsable de información sensitiva para resistir y reportar prácticas engañosas, tales como actividades sospechosas de hackers[6] y virus de computadoras.

[6] Ver Glosario

A.5	ROLES Y RESPONSABILIDADES DENTRO DE LA ORGANIZACIÓN
A.5.1	FUNCIÓN DE SEGURIDAD EN LA INFORMACIÓN
A.5.1.1	Establecer una función de Seguridad Informática en toda la empresa.
A.5.1.2	Asignar claramente y coordinar responsabilidades y obligaciones a todos los miembros de la Organización para apoyar la Función de Seguridad Informática.
A.5.1.3	Desarrollar y mantener una relación cooperativa con el personal de Seguridad Informática en la empresa y con otras organizaciones.

A.5.2	RESPONSABILIDAD SOBRE EL MANEJO DE LA INFORMACIÓN
A.5.2.1	Establecer una política dirigida a los responsables de los activos informáticos, que incluya asignaciones de propiedad, custodia y uso de la información.
A.5.2.2	Establecer un esquema de clasificación adecuada, que asigne los niveles de protección requeridos.
A.5.2.3	Desarrollar estándares, guías y procedimientos operativos de seguridad, para apoyar el registro de responsabilidades sobre los activos informáticos.
A.5.2.4	Definir y publicar sanciones por la falta de cumplimiento con estandares, lineamientos y procedimientos operacionales.
A.5.2.5	Otorgar premios y reconocimientos por desempeños de seguridad en la información.

A.5.3	ADMINISTRADORES Y COORDINADORES DE SEGURIDAD.
A.5.3.1	Designar y capacitar a coordinadores y administradores de Seguridad Informática en organizaciones descentralizadas.
A.5.3.2	Coordinar y establecer consistencia de actividades de seguridad descentralizadas a través de la función de Seguridad Informática .

A.5.4	AUTORIDAD LIMITADA.
A.5.4.1	Limitar el número de privilegios de autoridad asignados, de acuerdo con su responsabilidad de trabajo.
A.5.4.2	Deslindar responsabilidades o requerir acciones duales de quienes tienen autoridad a sistemas o transacciones privilegiadas a fin de que pudieran requerir de contubernio (asociación delictiva) para violar la seguridad.

A.5.5	SEGURIDAD EN LA DESCRIPCIÓN DE PUESTOS.
A.5.5.1	Incluir responsabilidades de Seguridad Informática en la descripción de puestos de los empleados.
A.5.5.2	Incluir incentivos en salario, desempeño y revisiones contractuales por el apego a políticas y participación con la Seguridad Informática.
A.5.5.3	Incluir funciones de control de entradas y salidas para la operación de producción y procesamiento de información.
A.5.5.4	Asegurar la separación de obligaciones y la clara definición de responsabilidades para todas las funciones de comunicación y proceso de información.

A.5.6	COMITÉ DE SEGURIDAD INFORMÁTICA.
A.5.6.1	Establecer un comité gerencial de Seguridad Informática responsable de la emisión de estrategias para toda la empresa incluyendo funciones de Seguridad Informática centralizada.

A.5.7	AUDITORÍA EN SISTEMAS.
A.5.7.1	Establecer la función de auditoría de sistemas de información como parte de la auditoría interna de la organización.
A.5.7.2	Establecer un amplio campo de responsabilidades de auditoría que estén en toda la empresa y cubran actividades computacionales centralizadas o descentralizadas.
A.5.7.3	Coordinar actividades de auditoría en los sistemas de información con la función de Seguridad Informática y definir responsabilidades de manera separada.

A.5.8	PERSONAL DE LA FUNCIÓN DE SEGURIDAD INFORMÁTICA.
A.5.8.1	Alentar la participación del personal de Seguridad Informática en actividades profesionales tales como obtener certificados de ISSA[7], ALAPSI[8], etc. (asociaciones que certifican a los profesionales en seguridad informática).
A.5.8.2	Suscribirse a las mejores publicaciones e instalar una biblioteca de libros, reportajes y diarios de Seguridad Informática.
A.5.8.3	Entrenar al personal de Seguridad Informática y hacerlos responsables de proteger la confidencialidad de la información de la seguridad.

[7] Information Systems Security Association, entidad norteamericana especialista en seguridad informática.
[8] Asociación Latinoamericana de Profesionales en Seguridad Informática.

A.6	AUTORIZACIONES, ACUERDOS Y CONTRATOS
A.6.1	**CONTRATOS.**
A.6.1.1	Establecer estipulaciones contractuales en conformidad con los proveedores de servicios sobre las políticas, normas y estándares de seguridad de la Organización.
A.6.1.2	Establecer estipulaciones contractuales y procedimientos de conformidad con el vendedor sobre aspectos de seguridad en productos y servicios adquiridos.
A.6.1.3	Incluir cláusulas sobre propiedad, confidencialidad y no divulgación de información en contratos de servicios.

A.6.2	AUTORIZACION DE USO
A.6.2.1	Obligar a todos los usuarios de información tecnológica a leer y reconocer las políticas sobre seguridad informática, el código de conducta y responsabilidades.
A.6.2.2	Solicitar autorización escrita para el uso de activos tecnológicos fuera de las instalaciones.

A.6.3	SEGUROS.
A.6.3.1	Incluir seguros para todos los activos informáticos como parte de un programa de protección.
A.6.3.2	Asegurar que los activos de información tecnológica sean cubiertos por planes de seguros o de prevención de riesgos.
A.6.3.3	Asegurar que todos los empleados de confianza sepan que serán vetados de acuerdo a la ley de prácticas industriales.

A.7	DESARROLLO Y ADQUISICIÓN DE SISTEMAS
A.7.1	**RESPONSABILIDADES EN EL DESARROLLO**
A.7.1.1	Incluir consideraciones de seguridad en el diseño y adquisición de toda la tecnología de información y contratos de outsourcing.[u]
A.7.1.2	Cumplir con las leyes y regulaciones en el desarrollo y mantenimiento de aplicaciones, operación y sistemas de comunicación.

[u] Como concepto general, es la contratación de los servicios de diferentes proveedores en lugar de tener funciones expresas dentro de la organización para la generación de dichos servicios

A.7.1.3	Desarrollar estándares de seguridad para el diseño de sistemas, que cubran todas las formas de tecnología de información (entradas, procesos, salidas, validaciones, consultas, etc.).
A.7.1.4	Asegurar que los usuarios, desarrolladores, seguridad informática y auditoria interna participen en la elaboración de estándares de seguridad para el desarrollo de sistemas.
A.7.1.5	Establecer una metodología formal de desarrollo de ciclo de vida de sistemas con procedimientos estándar
A.7.1.6	Establecer separadamente las librerías y archivos de programas en desarrollo de los de producción.
A.7.1.7	Usar controles de acceso y bitácoras de auditoría detalladas para proteger los programas de librerías y archivos.
A.7.1.8	Establecer procedimientos para verificar la consistencia de versiones de software y código fuente y ejecutable.
A.7.1.9	Mantener un sistema formal para el control de cambios que asegure que el hardware, software y servicios modificados, esten adecuadamente autorizados y documentados y que además los controles de seguridad sean preservados.
A.7.1.10	Almacenar los registros de el control de cambios y de reportes de problemas durante la vida completa del hardware y software.
A.7.1.11	Desarrollar y mantener documentación formal para todas las aplicaciones y sistemas de software que explícitamente identifique los controles de seguridad.

A.7.2	AMBIENTE DE PRUEBAS.
A.7.2.1	Mantener separados los ambientes y sistemas en producción de los de prueba.
A.7.2.2	Minimizar el uso de datos reales para pruebas.
A.7.2.3	Proteger la confidencialidad de los datos usados en pruebas de sistemas de aplicación.
A.7.2.4	Establecer un grupo independiente de control de calidad para pruebas y revisiónes de comunicaciones, software del sistema y aplicaciones críticas[10].

[10] Las aplicaciones críticas son aquellas que manejan información sensitiva y aquellas que sin el servicio, puede estar en peligro la existencia de la organización.

B) SEGURIDAD FÍSICA

Los siguientes controles deberán ser implementados por los responsables de la Función de Seguridad Informática de manera conjunta con las áreas involucradas, Auditoria Informática y con apoyo de la Dirección de la organización.

La siguiente tabla muestra los tópicos a considerar en la definición de políticas de seguridad física, éstos controles deberán ser revisados continuamente para evaluar su vigencia considerando aspectos técnicos y tecnológicos.

SEGURIDAD FÍSICA

- B.1 Localización de equipo.
- B.2 Control de acceso físico y cerraduras.
- B.3 Dispositivos removibles.
- B.4 Tecnología portátil.
- B.5 Construcciones.
- B.6 Autorización al acceso físico.
- B.7 Switch maestro de apagado eléctrico.
- D.7 Potencia eléctrica.

A continuación se describen a más detalle los controles a considerar para incrementar la seguridad física:

B.1	LOCALIZACIÓN DE EQUIPO.
B.1.1	Situar la información que se procesa y el equipo de comunicación, en localidades y construcciones que proporcionen protección contra daño, acceso y uso no autorizado.
B.1.2	Proporcionar un nivel adicional de seguridad para componentes críticos como cuartos y gabinetes cerrados.
B.1.3	Asegurar áreas sensitivas durante periodos no atendidos. (por ejemplo: áreas de manejo de efectivo, equipo de cómputo, laboratorios experimentales, etc.)
B.1.4	Asegurar líneas y equipo de comunicación.
B.1.5	Colocar las pantallas de las computadoras que despliegan información sensitiva fuera de la vista de personas no autorizadas.
B.1.6	Identificar las instituciones que pueden auxiliar en caso de emergencia, por ejemplo, cruz roja, policía, agencias civiles, centros de cómputo alterno, etc.
B.1.7	Separar la instalación de equipo de comunicaciones y diferentes tipos de equipo de cómputo en diferentes habitaciones tomando en cuenta los ambientes y accesos requeridos.

B.2	CONTROL DE ACCESO FÍSICO Y CERRADURAS.
B.2.1	Usar cerraduras físicas y/o dispositivos anti-robo en computadoras y equipos de comunicación incluyendo servidores, estaciones de trabajo y computadoras portátiles.
B.2.2	Incluir barreras físicas apropiadas en localidades clave para el acceso a las instalaciones, tal como entradas de construcciones, puntos sensitivos de áreas de acceso y cuartos con equipo de cómputo.
B.2.3	Incluir procedimientos controlados donde los puntos de acceso sean críticos, tal como vigilancia, recepción y control de entradas.

B.3	DISPOSITIVOS REMOVIBLES.
B.3.1	Desarrollar guías para el uso y control de dispositivos removibles cuando estén fuera de la corporación.
B.3.2	Asegurar los dispositivos removibles que contengan información crítica o sensitiva cuando no estén en uso, utilizando por ejemplo, cajas fuerte o gabinetes cerrados.
B.3.3	Proporcionar controles físicos adecuados y almacenamiento de registros para documentos negociables y otros documentos sensitivos, así como para el stock de formas negociables.

B.4	TECNOLOGÍA PORTÁTIL.
B.4.1	Mantener un inventario de todas las computadoras portátiles y otros dispositivos de tecnología portátil.
B.4.2	Aplicar marcas indelebles a activos permanentes, computadoras portátiles y otros dispositivos de tecnología portátil.
B.4.3	Ejecutar inventarios físicos de todo el equipo periódicamente.
B.4.4	Aplicar marcas únicas o colores a todos los dispositivos de almacenamiento removibles.

B.5	CONSTRUCCIONES.
B.5.1	Mantener características discretas de diseño para construcciones e instalaciones donde se guardan sistemas de cómputo y comunicaciones, por ejemplo evitar grandes símbolos de identificación.
B.5.2	Eliminar identificadores de las instalaciones de la empresa en donde se aloja equipo de cómputo crítico.
B.5.3	Mantener un perímetro seguro alrededor de todas las instalaciones, identificando instalaciones críticas las cuales requieran niveles más altos de seguridad y control.
B.5.4	Prohibir fumar y comer en centros de datos, áreas con proceso de información sensitiva y equipo de

	comunicaciones.

B.6	AUTORIZACIÓN AL ACCESO FÍSICO.
B.6.1	Identificar y documentar áreas con proceso de información crítica, sensitiva y actividades de comunicaciones.
B.6.2	Establecer y poner en práctica políticas de acceso limitado en áreas con actividades sensitivas.
B.6.3	Restringir las rutas de tráfico habitual para que éstas no interfieran con el equipo de comunicaciones y con el procesamiento de información sensitiva.
B.6.4	Solicitar a todos los empleados el uso de credenciales en áreas controladas.
B.6.5	Solicitar a todas las personas que no sean de la organización, tal como visitantes y contratistas, que usen distintivos de identificacion en áreas controladas.
B.6.6	Establecer requerimientos de identificacion para respuesta a emergencias, especificando procedimientos y responsabilidades individuales.

B.7	SWITCH MAESTRO DE APAGADO ELÉCTRICO.
B.7.1	Proporcionar un switch maestro de apagado y señalización de emergencia en lugares donde haya equipo electrónico, por ejemplo puertas de salida en instalaciones con equipo de cómputo.
B.7.2	Establecer servicios de informacion crítica en edificios que estén en localidades seguras con bajo índice de criminalidad, tráfico limitado y probabilidad mínima de incendios, inundaciones, vientos fuertes u otros eventos naturales extremos.
B.7.3	Proveer a todos los equipos de cómputo con proteccion eléctrica contra variaciones, fallas de potencia, y otras anomalías eléctricas.
B.7.4	Proporcionar un control de suspensión de energía eléctrica y controles de recuperación, tal como interruptores maestros de encendido colocados cerca de salidas de emergencia y fuentes de potencia alternativas para sistemas de cómputo críticos

C) SEGURIDAD EN COMUNICACIONES

En esta sección se proporciona una guía de los controles que se recomiendan sean implementados por la Función de Seguridad Informática junto con las áreas de sistemas distribuidos, redes, telecomunicaciones, etc. los cuales también deberán ser validados para establecer su nivel de obsolecencia y en su caso, deberán ser complementados con ayuda de las nuevas tecnologías.

La siguiente tabla muestra de manera global los tópicos que deberan ser considerados en la definición de políticas y controles para establecer niveles aceptables de seguridad en la parte de comunicaciones.

SEGURIDAD EN COMUNICACIONES

- C.1 Seguridad en redes.
- C.2 Autentificación de usuarios.
- C.3 Acceso remoto (dial-up).
- C.4 Criptografía ó encripción.
- C.5 Correo electrónico.
- C.6 Seguridad en sistemas distribuidos.
  - C.6.1 Red de area local (lan).
  - C.6.2 Aplicaciones distribuidas.
  - C.6.3 Seguridad en el server.
  - C.6.4 Autentificación cliente/servidor.
- C.7 Seguridad en sistemas de voz.
  - C.7.1 Protección en communicacion de larga distancia.
  - C.7.2 Protección de buzón de voz.
  - C.7.3 Monitoreo de llamadas.
- C.8 Seguridad en estaciones de trabajo.
  - C.8.1 Aislamiento de información sensitiva.
  - C.8.2 Control de acceso.
  - C.8.3 Eliminación de datos.

A continuación se detallan los controles a considerar:

C.1	SEGURIDAD EN REDES
C.1.1	Proteger el hardware y medios de comunicación contra intervenciones usando controles de acceso físico.
C.1.2	Usar controles de acceso lógicos para proteger dispositivos de red programables
C.1.3	Limitar el uso de herramientas de software especial (como los utilizados para el diagnóstico de red) al personal especificamente designado de acuerdo a sus responsabilidades de trabajo y almacenar de forma segura estas herramientas cuando no sean utilizadas.
C.1.4	Usar enlaces de comunicación a base de líneas dedicadas para estaciones de trabajo que tengan privilegios especiales o acceso a datos sensitivos en un ambiente host.
C.1.5	Limitar el acceso de toda la información de configuración de redes y los datos relacionados con seguridad tales como números privilegiados, direcciones de red (IP-address), rutas alternas, etc.
C.1.6	Proteger de acceso no autorizado los datos tales como vaciados de memoria(dumps), pruebas o

	vestigios de rutas o actividad (traces) y los archivos de datos de diagnósticos de red.
C.1.7	Mantener un control de las herramientas para la transferencia de archivos (E-Mail, File Transfer, etc.).
C.1.8	Verificar periódicamente cables y enlaces de comunicación para asegurarse de que no hay conexiones de equipo no autorizado.

C.2	AUTENTIFICACIÓN DE USUARIOS.
C.2.1	Utilizar sistemas de autentificación que permitan un seguro y único esquema de acceso maestro a múltiples sistemas.
C.2.2	Aplicar encripción a nivel de sesión para autentificar conexiones peer-to-peer y cliente/servidor
C.2.3	Usar técnicas de estampado encriptado basadas en fecha / hora y números de secuencias para prevenir la intercepción y repetición de mensajes sensitivos.
C.2.4	Usar los identificadores de teléfonos, modem o terminal como identificación y verificación complementaria de usuarios de la red, cuando estén disponibles.
C.2.5	Desplegar mensajes de advertencia de monitoreo y propiedad de la información en las pantallas iniciales o de entrada a la red.
C.2.6	Minimizar la información proporcionada al usuario antes de la autentificación, como no proporcionar información de la organización, sistema o red a la que se conectará, etc.
C.2.7	Usar "firewalls"[11], segmentación y controles de ruteo para protegerse de conexiones de red no autorizadas.
C.2.8	Usar menús, administradores de sesión y otros controles de ruteo de red para limitar el acceso de los usuarios solamente a aquellas aplicaciones de red para las que ellos han sido autorizados.
C.2.9	Desconectar físicamente todos los equipos de comunicación y segmentos de red que no sean necesarios.

C.3	ACCESO REMOTO (DIAL-UP).
C.3.1	Autentificar los usuarios vía dial-up con una capa de seguridad complementaria usando mecanismos de protección a puertos, tales como callback, autentificación de tokens o sistemas similares.
C.3.2	Usar mecanismos de autentificación que cubran toda la red WAN, como números automáticos de identificación (ANI) o grupos cerrados de usuarios (CUG) para verificar a los usuarios vía dial-up antes de su entrada (log-on).

[11] Ver Glosario

C.3.3	Mantener un sistema formal de autorización y registros para la asignación de líneas conmutadas para modems y máquinas de fax que serán puestos dentro de las instalaciones de la organización
C.3.4	Usar pools[12] de servidores/modems de comunicación en lugar de estaciones de trabajo individuales con puertos de acceso dial-up.

C.4	CRIPTOGRAFÍA O ENCRIPCIÓN
C.4.1	Aplicar encripción, códigos de autentificación de mensajes y firmas digitales para proteger comunicaciones sensitivas.
C.4.2	Proteger transmisiones de microondas y satelitales con encripción de enlace
C.4.3	Establecer sistemas de administración de llaves que garanticen una distribución segura y a tiempo de llaves de encripción.

C.5	CORREO ELECTRÓNICO.
C.5.1	Comunicar las políticas de la organización en materia de uso y privacidad del correo electrónico, monitoreo y un adecuado contenido de advertencias de las vulnerabilidades.
C.5.2	Limitar el acceso de los usuarios de correo electrónico al envío y recepción de mensajes de correo únicamente dentro de las aplicaciones de red que le atañen, a menos que los usuarios hayan sido específicamente autorizados para usar otras aplicaciones.

C.6	SEGURIDAD EN SISTEMAS DISTRIBUIDOS[13]
C.6.1	RED DE AREA LOCAL (LAN).
C.6.1.1	Utilizar tarjetas adaptadoras LAN que no permitan el uso, desde las estaciones de trabajo, de software que pueda interceptar paquetes de mensajes y datos en la red.
C.6.1.2	Evitar el uso de sistemas operativos de LANs punto a punto en redes de gran tamaño y/o aplicaciones sensitivas.
C.6.1.3	Usar encripción para proteger mensajes sobre todas las LANs con tecnología de radiofonía

[12] Grupo o combinación de periféricos.

[13] Denominamos a los sistemas de computación distribuida a aquellos que utilizan redes de computadoras en las que una o más maquinas se encuentran conectadas a un procesador central y que en este tipo de redes, todos los procesos y datos son cargados a partir del procesador que controla la red; como un ejemplo de este tipo de sistemas se puede mencionar la redes LAN. Por otro lado, también encontramos redes generalmente de proporciones mucho mayores a las anteriores en la que los procesos, datos o aplicaciones residen en diferentes procesadores (CPU's), a los que cada maquina puede acceder y procesar la información que resida en este lugar.
Las aplicaciones o sistemas distribuidos, la tecnología cliente-servidor y las bases de datos distribuidas son todas las variantes y componentes de un "sistema distribuido"

	infrarroja (tecnología de reciente uso).
C.6.1.4	Utilizar cable blindado a lo largo de rutas seguras para minimizar la interferencia y monitoreo no autorizado de redes de comunicación

C.6.2	APLICACIONES DISTRIBUIDAS.[14]
C.6.2.1	Construir servicios de seguridad dentro de las aplicaciones distribuidas usando los estándares de Interfases de Programas de Aplicación (API)
C.6.2.2	Usar múltiples definiciones de interfases de seguridad como verificadores de integridad y confidencialidad, en el mismo punto de verificación para evitar tareas repetitivas de chequeo de la seguridad.
C.6.2.3	Aplicar controles para obtener transacciones "bien formadas"[15], y para verificar la autenticidad e integridad en los datos antes y después del proceso.
C.6.2.4	Proteger todos los recursos distribuidos sensitivos con listas de control de acceso (ACLs)[16], localizados dentro del mismo nodo.
C.6.2.5	Limitar el acceso directo a las interfases entre aplicaciones y otros interprocesos privilegiados de comunicaciones, solamente a usuarios y procesos autorizados.
C.6.2.6	Aplicar encripción para proteger los datos que se transfieren entre el cliente y el servidor, basándose en la sensitividad de las aplicaciones.

[14] En este tipo de aplicaciones o sistemas distribuidos tanto los datos como las aplicaciones se encuentran dispersas a través de todo el hardware del sistema existiendo entre ellos una relación de interdependencia y los cuales son implementados mediante llamadas a procesos remotos (RPC/Remote Procedure Call).

[15] Transacciones consistentes, íntegras y completas

[16] Access Control List (ACL's), son relaciones en donde se especifica que tipo de permiso o acceso tendrá a diferentes recursos del sistema.

C.6.3	SEGURIDAD EN EL SERVER.
C.6.3.1	Segmentar las redes y aplicaciones distribuidas en diferentes nodos con servidores dedicados.
C.6.3.2	Usar servidores separados para cada servicio o función principal, tal como seguridad, servicios de tiempo distribuido, servidores de archivos, y administración de redes
C.6.3.3	Usar servidores de seguridad en lugar de almacenar información sobre cada estación de trabajo.
C.6.3.4	Instalar múltiples servidores de seguridad, en aplicaciones de gran tamaño o aplicaciones multi-nodos.
C.6.3.5	Usar múltiples servidores con servicios de tiempo distribuidos (DTS), tomando en cuenta el tamaño de la red, para asegurar el tiempo de sincronización.
C.6.3.6	Proporcionar seguridad a la base de datos a través de servicios de distribución y actualización para aplicaciones con múltiples servidores de seguridad.
C.6.3.7	Limitar el acceso físico a todos los servidores y proporcionar protección contra fuego, agua, alteraciones de corriente y fallas mecánicas.
C.6.3.8	Aplicar controles de acceso lógico para limitar el acceso a los servidores.

C.6.4	AUTENTIFICACIÓN CLIENTE/SERVIDOR.
C.6.4.1	Establecer procedimientos homogeneos de autentificación inter-nodos que sean verificados y aceptados por cada administrador de seguridad del nodo.
C.6.4.2	Proporcionar verificación en ambos sentidos para asegurar que la autentificación del cliente y del servidor son mutuamente reconocidas.
C.6.4.3	Minimizar la re-autentificación de usuarios asignando tickets especialmente encriptados, tales como los que usa el sistema Kerberos[17].
C.6.4.4	Definir lapsos de vida del ticket[18] y frecuencia de re-autentificación, basados en la sensitividad de aplicaciones afectadas.
C.6.4.5	Aplicar llaves de conversación como un sustituto seguro de llaves secretas cuando un usuario / cliente se comunica con cada servidor.
C.6.4.6	Definir frecuencias aceptables para la re-autentificación de llamadas de procedimiento remoto (RPC's[19]), basadas en la sensitividad de las aplicaciones afectadas.

[17] Ver Glosario
[18] Ver Kerberos en el glosario
[19] Remote Procedure Calls

C.7	SEGURIDAD EN SISTEMAS DE VOZ
C.7.1	**PROTECCIÓN EN COMUNICACION DE LARGA DISTANCIA**
C.7.1.1	Limitar el acceso a servicios de larga distancia a usuarios autorizados y estaciones telefónicas
C.7.1.2	Usar tarjetas de crédito con servicios de larga distancia como una alternativa al uso del número 800 que tiene acceso dial-in, dial-out, para evitar la observación por parte de terceros en lugares públicos, de las claves de acceso.
C.7.1.3	Proteger todas las líneas de sistemas de acceso directos hacia el interior, usando la máxima longitud de password permitida por el sistema.
C.7.1.4	Usar características de bloqueo de llamadas para prevenir llamadas no deseadas de localidades prohibidas (códigos de áreas, claves lada) y apagar durante periodos específicos.
C.7.1.5	Aplicar procedimientos adecuados de manejo automático de errores para todos los conmutadores y sus componentes de soporte, como atención de llamadas para prevenir fallas a través de accesos a largas distancias.

C.7.2	PROTECCIÓN DE BUZÓN DE VOZ.
C.7.2.1	Usar passwords bien elegidos con controles administrativos estándar para proteger la voz de buzones
C.7.2.2	Desactivar todos los buzones de voz no usados.

C.7.3	MONITOREO DE LLAMADAS.
C.7.3.1	Implementar reportes detallados de llamadas.
C.7.3.2	Monitorear regularmente la actividad de llamadas a conmutadores de larga distancia.
C.7.3.3	Deshabilitar todas las funciones de administración remota a través de las teclas del teléfono de los conmutadores.
C.7.3.4	Adherir controles de acceso lógico y físico para proteger los componentes de cómputo de los sistemas de conmutación.
C.7.3.5	Desactivar el modem o usar passwords basados en tokens para proteger el acceso dial-up a los puertos del conmutador.

C.8	SEGURIDAD EN ESTACIONES DE TRABAJO
C.8.1	**AISLAMIENTO DE INFORMACIÓN SENSITIVA.**
C.8.1.1	Usar medios removibles para almacenar información sensitiva fuera de línea, en lugar de usar control de acceso para datos almacenados permanentemente en discos duros.
C.8.1.2	Proporcionar un estricto control físico, como gabinetes cerrados o cajas fuertes, para datos sensitivos almacenados sobre medios removibles.
C.8.1.3	Usar servidores de archivos y otros sistemas seguros "centralizados" en lugar de estaciones de trabajo para almacenar información sensitiva y/o crítica.

C.8.2	CONTROL DE ACCESO.
C.8.2.1	Usar hardware contra robo y ataques junto con otras medidas de seguridad físicas para proteger estaciones de trabajo de escritorio y portátiles contra robo e intrusión.
C.8.2.2	Usar firmware[20] y/o características de control de acceso lógico y físico para prevenir el uso no autorizado de estaciones de trabajo.
C.8.2.3	Usar características de control de acceso al software, tal como listas de control de acceso y encripción, para restringir selectivamente el acceso a información sensitiva.
C.8.2.4	Usar firmware y/o características de control de acceso al software para prevenir el acceso no autorizado a datos de la estación de trabajo a través de puertos de entrada/salida.
C.8.2.5	Usar firmware y/o características de control de acceso al software cuando sea factible crear "estaciones de trabajo diskless[21] " para prevenir la eliminación no autorizada y entradas de software y datos a través de la estación de trabajo.
C.8.2.6	Monitorear y actualizar los niveles de protección para las aplicaciones de estaciones de trabajo controladas centralmente.
C.8.2.7	Eliminar o limitar el uso y asignación de estaciones de trabajo privilegiadas.

[20] Micropiogramación cableada, es decir, programación de chips o memorias para funciones específicas.
[21] Estaciones de trabajo sin unidad de floppy y disco duro.

C.8.3	ELIMINACIÓN DE DATOS.
C.8.3.1	Borrar electromagnéticamente los medios de almacenamiento usando técnicas de eliminación completas, tal como ceros binarios o datos aleatorios, antes de almacenar y/o transferir la custodia de estaciones de trabajo y servidores que contengan información sensitiva.
C.8.3.2	Proporcionar y usar dispositivos de eliminación (neutralización del campo magnético) para medios magnéticos.
C.8.3.3	Practicar la destrucción completa de medios de almacenamiento cuando éste o su contenido ya no sean utilizados.

D) SEGURIDAD LÓGICA

Los presentes controles son los más importantes desde la perspectiva de la seguridad en la información y deben ser complementados con los mencionados en las secciones anteriores (políticas, seguridad física y seguridad en comunicaciones). Estos controles básicos deberán ser implementados con el esfuerzo de todas las áreas de la organización que requieran ser incrementados sus niveles de seguridad y es muy importante la participación y apoyo de la alta dirección en el otorgamiento de recursos (presupuestos para adquisición de nueva tecnología, personal, concientización y difusión, etc.).

Para asegurar la correcta protección de la información y una administración efectiva, se deben diseñar estándares de seguridad para proteger todos los requerimientos importantes, es decir, se deben tomar en cuenta:

- Identificación y Autentificación de usuarios
- Controles en la autoridad de privilegios
- Encripción
- Disuasivos por intrusión
- Controles en la integridad y autenticidad de software
- Administración y configuración de la seguridad
- Autorización de acceso a datos
- Bitácoras de seguridad/auditoria
- Documentación

La siguiente tabla menciona los controles a considerar para el incremento de la seguridad lógica:

SEGURIDAD LÓGICA

- D.1 Administración de la seguridad.
- D.2 Protección de datos y sistemas.
- D.3 Auditorias y revisiones.
- D.4 Análisis de riesgos y reportes de pérdidas.
- D.5 Control y destrucción de documentos.
- D.6 Operación en condiciones de emergencia.
- D.7 Identificación y autentificación de usuarios
  - D.7.1 Administración de identificadores de usuario.
  - D.7.2 Administración de claves de acceso.
  - D.7.3 Detención de intrusos.
  - D.7.4 Reautentificación de transacciones sensitivas.
  - D.7.5 Tokens para autentificación.
  - D.7.6 Biométricas y firmas digitales.
  - D.7.6.4 Procedimientos de emergencia y excepción.
- D.8 Bitácoras de seguridad y monitoreo
  - D.8.1 Monitoreo de eventos relacionados con seguridad.
  - D.8.2 Monitoreo del sistema y la aplicación de seguridad.
- D.9 Protección contra software dañino
  - D.9.1 Políticas y procedimientos.
  - D.9.2 Convenios.
  - D.9.3 Software anti-virus.
  - D.9.4 Procedimientos de respaldo y emergencia.
  - D.9.5 Reporte de incidencias de software contaminado.
- D.10 Respaldos y recuperación
  - D.10.1 Planes de recuperación del negocio.

D.10.2 Simulacros de recuperación del negocio.
D.10.3 Tolerancia a fallas.
D.10.4 Respaldos y almacenamiento alterno.
D.10.5 Respaldos de servidores y estaciones de trabajo.
D.10.6 Servicios y equipo para recuperación en contingencias.
D.10.7 Contingencia financiera.
D.11 Administración y configuración de software
D.11.1 Directrices administrativas.
D.11.2 Revisión de niveles de cumplimiento.
D.11.3 Licencias de software y control de versiones.
D.11.4 Protección contra copias.

A continuación se detallan los controles a incluir:

D.1	ADMINISTRACIÓN DE LA SEGURIDAD.
D.1.1	Asignar administradores de seguridad para cada plataforma (hosts, redes, cliente/servidor).
D.1.2	Proporcionar la separación de responsabilidades entre individuos que son responsables del soporte técnico y la administración de seguridad.
D.1.3	Usar software de control de acceso para proporcionar protección a sistemas de software e información, el software debe tener seguridad de acuerdo con los criterios aceptados por organismos internacionales especialistas en estos rubros.[22]
D.1.4	Usar la característica de administración de usuarios del software de control de acceso, para reducir errores y para minimizar la administración y sobrecarga del sistema.
D.1.5	Proporcionar capacitación a los administradores de seguridad en el uso apropiado del software y mecanismos de seguridad.
D.1.6	Asignar responsabilidades a los propietarios, custodios y usuarios de activos informáticos como parte de las políticas.
D.1.7	Cambiar passwords o desactivar identificadores de usuarios de proveedores, cuando finalicen sus obligaciones.
D.1.8	Proteger el software del sistema y otros recursos sensitivos de seguridad tomando en cuenta las especificaciones y recomendaciones del proveedor.
D.1.9	Asignar atributos privilegiados solamente a un número limitado de usuarios y programas autorizados.
D.1.10	Utilizar procedimientos de control de acceso para limitar el uso de utilerías poderosas de software y herramientas de diagnóstico al personal de soporte capacitado, el uso de utilerías debe ser consistente con sus responsabilidades de trabajo.
D.1.11	Hacer una selección auditable de opciones de seguridad disponibles en el sistema, para el administrador del mismo, durante la carga inicial del equipo.

[22] Por ejemplo el Federal Criteria/CISR

D.1.12	Ejecutar periódicamente pruebas de integridad de controles de acceso (vigencia y validéz) y de las características de diagnóstico para el software del sistema.

D.2	PROTECCIÓN DE DATOS Y SISTEMAS.
D.2.1	Usar listas de control de acceso para proteger el software del sistema, las aplicaciones, los datos y alguna otra información valiosa de los recursos del sistema.
D.2.2	Establecer un acceso por default con privilegios de sólo lectura para el caso de no existir esquemas de asignación de privilegios.
D.2.3	Limitar el número, registro histórico y posesión de copias de información sensitiva.
D.2.4	Usar computadoras aisladas/dedicadas para la mayor parte de las aplicaciones sensitivas, cuando amenazas potenciales justifiquen esta acción.
D.2.5	Restringir el acceso de los usuarios a los datos de las aplicaciones sensitivas, a través de programas y/o transacciones específicas.
D.2.6	Prevenir jobs calendarizados y demonios[23], para no obtener más privilegios de acceso que los ya definidos y autorizados.
D.2.7	Establecer restricciones sobre los privilegios de información desplegados.
D.2.8	Establecer controles de acceso a archivos de datos por funciones de trabajo.
D.2.9	Definir responsabilidades para el control de programas de aplicación
D.2.10	Aplicar características del software de control de acceso que limiten la hora del día, el día de la semana y la localidad de la red para sistemas sensitivos y/o aplicaciones.
D.2.11	Aplicar características de eliminación completa (controles de reuso de objetos) para medios de almacenamiento públicos que contengan información sensitiva.
D.2.12	Evitar etiquetas externas descriptivas sobre medios de almacenamiento removibles
D.2.13	Usar "candados" mientras utiliza accesos simultáneos a bases de datos.
D.2.14	Usar registros de controles de transacciones "bien formadas" y separación de responsabilidades, como los que se presentan en el Modelo de Integridad de Clark-Wilson[24]
D.2.15	Emplear controles de acceso para estaciones de trabajo móviles como una base para limitar el acceso a sistemas y/o aplicaciones sensitivas.
D.2.16	Controlar el uso de estaciones de trabajo con programas que permitan la carga y descarga de información del host a programas y usuarios específicos.

[23] Los "demons" son procesos que corren en background (en ambiente multitarea), permitiendo que el ambiente de foreground (comandos o procesos en línea) continúe sin darse cuenta de que se está corriendo otro proceso en el mismo instante.

[24] En el modelo de Clark Wilson las transacciones y datos "well-formed" no pueden ser manipulados por el usuario en forma arbitraria, conservando así, su integridad y reduciendo el riesgo de pérdida o corrupción de datos.

D.3	AUDITORIAS Y REVISIONES.
D.3.1	Ejecutar periódicamente auto-evaluaciones de seguridad informática , usando listas de verificación (checklist), escalas de comparación u otras medidas.
D.3.2	Llevar a cabo regularmente inspecciones de los sistemas de información.
D.3.3	Llevar a cabo inspecciones sorpresivas de seguridad en sistemas de información, tales como exploraciones en horas inhábiles.
D.3.4	Ejecutar auditorias de sistemas de información conducidas por auditores internos o externos.
D.3.5	Clasificar y proteger adecuadamente los reportes de auditoria y seguridad.
D.3.6	Reportar a los niveles apropiados, discrepancias y deficiencias de seguridad que se identifiquen en las revisiones o auditorias.
D.3.7	Mantener registros de anomalías por periodos definidos en las políticas de retención y almacenamiento de información interna.
D.3.8	Realizar revisiones periodicas por especialistas de seguridad informática de la información de uso intensivo de la organizacion.

D.4	ANÁLISIS DE RIESGOS Y REPORTES DE PÉRDIDAS.
D.4.1	Solicitar reportes de todos los incidentes relacionados a la seguridad informática .
D.4.2	Mantener una base de datos de incidentes internos y externos de seguridad informática por un periodo considerable.

D.5	CONTROL Y DESTRUCCIÓN DE DOCUMENTOS.
D.5.1	Establecer procedimientos de confirmacion para recibir documentos importantes.
D.5.2	Establecer procedimientos de eliminación de datos incompletos y obsoletos.
D.5.3	Destruir documentos cuando no sean requeridos por razones legales y de operación.
D.5.4	Establecer procedimientos de manejo de desperdicios.
D.5.5	Establecer procedimientos para control de documentos e impresiones.
D.5.6	Marcar documentos e impresiones con una clasificación apropiada.
D.5.7	Inspeccionar el material que entra y sale de áreas sensitivas.

D.6	OPERACIÓN EN CONDICIONES DE EMERGENCIA.
D.6.1	Establecer procedimientos de operacion especial para el control de aplicaciones en condiciones de emergencia.

D.6.2	**Incorporar un sistema para la administración de medios removibles cuando las operaciones incluyan un uso importante de los mismos.**

D.7	**IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS**
D.7.1	**ADMINISTRACIÓN DE IDENTIFICADORES DE USUARIO.**
D.7.1.1	**Proporcionar identificadores de usuario únicos para cada usuario y/o proceso automatizado.**
D.7.1.2	**Verificar la identidad de cada usuario a través de un buen método de autentificación, tal como un esquema apropiado de passwords secretos.**
D.7.1.3	**Proporcionar procedimientos para delegar identificadores de usuarios que permitan mantener registros individuales, cuando un usuario sea autorizado para actuar en representación de otros, (tal como un empleado actuando en representación de su gerente**
D.7.1.4	**Usar información de autentificación adicional para verificar la identidad de los usuarios antes de cambiar su password.**
D.7.1.5	**Proporcionar un método seguro para el inicio de sesión y mantenimiento de toda la información de identificación y autentificación.**
D.7.1.6	**Garantizar un proceso de registro seguro, incluyendo el envío o entrega al usuario de su clave de acceso inicial y la verificación de identidad del usuario.**
D.7.1.7	**Minimizar y eliminar, al máximo posible, el uso de cuentas de usuarios huésped (guest).**
D.7.1.8	**Limitar la distribución de documentación en línea o impresa y manuales concernientes a procedimientos de acceso.**
D.7.1.9	**Minimizar o eliminar la posibilidad de entradas simultáneas al sistema por el mismo identificador de usuario desde diferentes direcciones de red o estaciones de trabajo.**
D.7.1.10	**Establecer una estricta autentificación y autorización para los administradores de seguridad, administradores del sistema y otros usuarios privilegiados.**
D.7.1.11	**Proteger los archivos que contienen los passwords con control de acceso y encripción.**
D.7.1.12	**Proteger los archivos de passwords contra remoción, acceso directo y copiado, usando archivos sombra (shadows).**
D.7.1.13	**Proteger la comunicación de los procedimientos de acceso con encripción.**

D.7.2	ADMINISTRACIÓN DE CLAVES DE ACCESO.
D.7.2.1	Comunicar los requerimientos y sanciones para tratar de minimizar que los usuarios compartan sus claves de acceso y divulguen información no autorizada de sus identificadores de usuarios.
D.7.2.2	Establecer y ejecutar requerimientos reguladores del contenido del password, longitud y frecuencia de cambio.
D.7.2.3	Solicitar a los usuarios cambiar sus passwords sobre bases periódicas con re-autentificación.
D.7.2.4	Desplegar la última fecha y hora de acceso después de un acceso válido.

D.7.3	DETECCIÓN DE INTRUSOS.
D.7.3.1	Forzar la desconexión de sesión o inhabilitar la entrada de un dispositivo despues de un periodo especifico de inactividad.
D.7.3.2	Limitar el número y frecuencia de intentos de acceso no validos.
D.7.3.3	No proporcionar información referente a los limites y acciones tomadas sobre intentos de acceso no exitosos.

D.7.4	REAUTENTIFICACIÓN DE TRANSACCIONES SENSITIVAS.
D.7.4.1	Proporcionar restricciones de acceso a aplicaciones sensitivas por hora del dia, día de la semana, terminales especificas y otras condiciones seleccionadas.
D.7.4.2	Re-autentificar el usuario cada vez que una transaccion altamente sensitiva sea requerida.

D.7.5	TOKENS[25] PARA AUTENTIFICACIÓN.
D.7.5.1	Usar tokens que generen un nuevo código de autentificación aleatorio o password en cada uso.
D.7.5.2	Restringir el uso y posesion de cada token a un solo usuario.
D.7.5.3	Asignar adicionalmente un numero de identificacion personal secreto o un password para usar con tokens.
D.7.5.4	Mantener un inventario seguro de controles para la asignación de dispositivos token.
D.7.5.5	Requerir el regreso de tokens a la terminación del empleo o reasignación de funciones que no requieren el uso de los mismos.

[25] Un token o ficha, es aquel elemento o dispositivo utilizado para proporcionar un nivel superior de autenticidad.

D.7.6	BIOMÉTRICAS Y FIRMAS DIGITALES.
D.7.6.1	Usar biometricas[26] para autentificación de usuarios donde sea apropiado.
D.7.6.2	Establecer límites de falsa aceptación y falso rechazo en la autentificación por medio de biométrica.
D.7.6.3	Proteger transacciones sensitivas y datos con firmas digitales.

D.7.6.4	PROCEDIMIENTOS DE EMERGENCIA Y EXCEPCIÓN.
	Establecer un plan de contingencias en caso de que el mecanismo de autentificación o el subsistema de autorización falle.

D.8	BITÁCORAS DE SEGURIDAD Y MONITOREO
D.8.1	MONITOREO DE EVENTOS RELACIONADOS CON SEGURIDAD.
D.8.1.1	Equipar a todos los sistemas multi-usuarios con las características completas de las bitácoras de seguridad definidas por las autoridades competentes.
D.8.1.2	Activar las características de seguridad de las bitácoras para registrar todos los eventos importantes de seguridad, incluyendo los intentos de acceso: fallidos y exitosos.
D.8.1.3	Ejecutar revisiones periódicas y dar seguimiento de los eventos excepcionales señalados en los reportes de las bitácoras de seguridad.
D.8.1.4	Guardar los registros de las bitácoras de seguridad durante los periodos requeridos por la autoridad competente.
D.8.1.5	Usar utilerías de detección automatizadas en tiempo real para monitorear desviaciones significativas con respecto a la actividad normal y alertar a los administradores de seguridad en aplicaciones de alto riesgo.
D.8.1.6	Proveer control de acceso y pistas de auditoria a cualquier proceso que se imponga que pase por encima de la seguridad implantada.
D.8.1.7	Recompensar buenas practicas de seguridad y tomar acciones correctivas para violaciones.

[26] Un biometrica se conoce en seguridad como aquel elemento que varía en cada ser humano, por ejemplo, huellas digitales, contorno del rostro, iris del ojo, voz, etc.

D.8.2	MONITOREO DEL SISTEMA Y LA APLICACIÓN DE SEGURIDAD.
D.8.2.1	Revisar, desactivar y remover cuentas de usuarios inactivos en un periodo de tiempo.
D.8.2.2	Notificar inmediatamente a los administradores de seguridad de terminación de contratos, despidos y transferencias de empleados, contratistas y/o proveedores y otros usuarios de aplicaciones.
D.8.2.3	Coordinar revisiones periódicas de privilegios de acceso por los administradores de seguridad y los propietarios de la información.
D.8.2.4	Revisar y remover todos los datos y software inactivo periódicamente.

D.9	PROTECCIÓN CONTRA SOFTWARE DAÑINO

D.9.1	POLÍTICAS Y PROCEDIMIENTOS.
D.9.1.1	Emitir políticas y procedimientos para la protección y recuperación contra la contaminación de software nocivo.
D.9.1.2	Publicar políticas y procedimientos acerca del uso y medidas de seguridad contra software de dudosa confiabilidad.

D.9.2	CONVENIOS.
D.9.2.1	Probar todo el software obtenido de fuentes externas para asegurar su confiabilidad y autenticidad, y para identificar código defectuoso o nocivo.
D.9.2.2	Asegurar que todo el software que va a ser usado esté soportado y acompañado de su código fuente correspondiente y su respectiva documentación
D.9.2.3	Usar software de verificación de integridad automática (CRC, Checksum) para preservar la integridad del software y para detectar cambios y/o reemplazos no autorizados.

D.9.3	SOFTWARE ANTI-VIRUS.
D.9.3.1	Usar software anti-virus para detectar la posible presencia de virus en todo el software, diskettes, y sistemas de cómputo recientemente adquiridos, sin importar la fuente.
D.9.3.2	Usar cuarentena junto con software anti-virus para verificar la presencia de software nocivo en software y diskettes.
D.9.3.3	Usar software de control de acceso y procedimientos de control de cambios adicionalmente al software anti-virus para prevenir la introducción de software no autorizado.

D.9.4	PROCEDIMIENTOS DE RESPALDO Y EMERGENCIA.
D.9.4.1	Mantener una copia original de la versión actual de software, además de los respaldos regulares calendarizados.
D.9.4.2	Definir procedimientos de respuesta ante emergencias, incluyendo un equipo de respuesta a emergencias, para proceder en incidentes de software contaminado.

D.9.5	REPORTE DE INCIDENCIAS DE SOFTWARE CONTAMINADO.
D.9.5.1	Reportar todos los incidentes de software contaminado al soporte técnico y a las organizaciones de seguridad adecuadas.
D.9.5.2	Mantener archivos de incidentes de software contaminado para usar en análisis, en programas de concientización y capacitación.

D.10	RESPALDOS Y RECUPERACIÓN

D.10.1	PLANES DE RECUPERACIÓN DEL NEGOCIO.
D.10.1.1	Desarrollar y documentar planes de continuidad del negocio de carácter corporativo.
D.10.1.2	Desarrollar y documentar planes de continuidad del negocio para aplicaciones críticas.
D.10.1.3	Documentar planes de recuperación de desastres para centros de cómputo.
D.10.1.4	Asignar responsabilidades individuales para continuidad del negocio.

D.10.2	SIMULACROS DE RECUPERACIÓN DEL NEGOCIO.
D.10.2.1	Probar regularmente todos los planes de recuperación de desastres y de continuidad del negocio.
D.10.2.2	Incluir a los usuarios adecuados del negocio, auditores internos y staff de seguridad informática como parte del equipo de pruebas de planes de continuidad del negocio.

D.10.3	TOLERANCIA A FALLAS.
D.10.3.1	Asegurar la continuidad de la operacion de aplicaciones criticas usando computadoras con tolerancia a fallas o diseño redundante, incluyendo procesadores duplicados, discos espejos, bitácoras de transacciones de acceso y reguladores de voltaje (UPS).
D.10.3.2	Usar rutas alternas de comunicación para asegurar la disponibilidad de las comunicaciones.

D.10.4	RESPALDOS Y ALMACENAMIENTO ALTERNO.
D.10.4.1	Contar con un respaldo fuera del centro de cómputo (site) de al menos 2 copias o generaciones de todos los datos.
D.10.4.2	Establecer una calendarización regular para respaldos.
D.10.4.3	Proteger los medios en los que se encuentran los respaldos en tránsito, así como en el lugar donde se generan.
D.10.4.4	Establecer sites de almacenamiento de respaldos que no sean susceptibles a los mismos desastres que los que el centro de cómputo primario pueda experimentar.

D.10.5	RESPALDOS DE SERVIDORES Y ESTACIONES DE TRABAJO.
D.10.5.1	Efectuar respaldos de los sistemas completo desde su instalación inicial y dar seguimiento a cualquier cambio en servidores, estaciones de trabajo y medios removibles.
D.10.5.2	Ejecutar respaldos periódicos para servidores, estaciones de trabajo y medios removibles.
D.10.5.3	Utilizar procedimientos de respaldo, por ejemplo, respaldar los datos de la estación de trabajo en el servidor.
D.10.5.4	Desarrollar planes de preparación contra emergencias para todas las instalaciones del negocio.

D.10.6	SERVICIOS Y EQUIPO PARA RECUPERACIÓN EN CONTINGENCIAS.
D.10.6.1	Desarrollar alternativas de suministro de energía para edificios e instalaciones, principales centros de datos y sistemas distribuidos críticos.
D.10.6.2	Obtener el compromiso de los proveedores para reemplazar y proporcionar equipo durante una recuperación de contingencia después de una pérdida.
D.10.6.3	Adquirir y probar periódicamente el equipo de comunicaciones móvil para usar en situaciones de emergencia.
D.10.6.4	Contratar preventivamente servicios de recuperación externos o establecer sites de soporte mutuo.

D.10.7	CONTINGENCIA FINANCIERA.
D.10.7.1	Establecer fuentes adecuadas de financiamiento y efectivo como parte del plan de contingencias para el negocio.

D.11	ADMINISTRACIÓN Y CONFIGURACIÓN DE SOFTWARE

D.11.1.	DIRECTRICES ADMINISTRATIVAS.
D.11.1.1	Emitir y ejecutar políticas que prohiban el uso inadecuado de licencias de software y derechos reservados.
D.11.1.2	Obligar el uso de productos estándares de hardware y software como base principal para adquisiciones de tecnología de información.
D.11.1.3	Incluir la cobertura del software con derechos reservados y emitir licencias como parte de los programas de concientización de seguridad.

D.11.2	REVISIÓN DE NIVELES DE CUMPLIMIENTO.
D.11.2.1	Asignar los departamentos de gestión como puntos de control para asegurar el apego con las políticas de seguridad relacionadas con la adquisición.
D.11.2.2	Ejecutar inventarios periódicos de activos tecnológicos, tal como estaciones de trabajo de escritorio, laptops y software técnico.
D.11.2.3	Notificar a las autoridades apropiadas y verificar las investigaciones concernientes al hardware y software extraviado.
D.11.2.4	Utilizar auditorías o software de administración de configuración para monitorear el apego con las políticas y los estándares de la organización, incluyendo software con derechos reservados y licencias.

D.11.3	LICENCIAS DE SOFTWARE Y CONTROL DE VERSIONES.
D.11.3.1	Mantener pruebas de compra de todas las copias de software comercial utilizado por la empresa.
D.11.3.2	Optimizar el uso de licencias corporativas para reducir la probabilidad de copias de software no autorizadas.
D.11.3.3	Controlar y actualizar las bitácoras del software existente.
D.11.3.4	Actualizar el software de aplicación en sistemas distribuidos automáticamente desde un sistema de cómputo centralizado.

D.11.4	**PROTECCIÓN CONTRA COPIAS.**
D.11.4.1	**Utilizar características de solo-ejecución en el software de control de acceso para prevenir copias no autorizadas de software propietario.**

CAPITULO VI

ANALISIS DE RIESGOS

Cuando consideramos la compra y la utilización de un producto de seguridad, se tiene que balancear el costo del producto contra el riesgo de trabajar sin éste. Algunas organizaciones formalizan este proceso y lo denominan Análisis de Riesgos. El Análisis de Riesgos es un procedimiento utilizado para estimar las pérdidas potenciales que pueden resultar de un sistema vulnerable y para cuantificar el daño que resulte si ciertas amenazas se materializan. La última meta del análisis de riesgos es la de ayudar a seleccionar en base a un costo-beneficio, medidas de seguridad que reducirán los riesgos a un nivel aceptable; básicamente, el análisis de riesgos es una manera de valorar que tan importante es un determinado sistema y que tan lejos o no se esta (en términos de equipo, personal y presupuesto) de protegerlo.

El análisis de riesgos estándar involucra los activos tangibles, como son, edificios, equipo de cómputo, y demás equipamiento; y visualiza como están protegidos. Debido a que en cualquier Organización el activo más importante después del personal, es la información procesada por las computadoras, no las computadoras por si mismas, necesitamos identificar la mejor manera de proteger dicha información.

Cuando se están evaluando los activos de información de la organización considerando cuando y como protegerla, surgen una serie de interrogantes que responder:

- *¿Qué información se tiene y que tan importante es?*

  Como se explicó en Capitulo III con respecto a la clasificación de la información, sabemos que existen diferentes tipos de información: información de la Defensa Nacional la cual describiría recursos, tácticas y despliegues militares; registros corporativos mostrando pérdidas y estrategias de mercado; registros personales describiendo enfermedades, estados financieros, cuestiones académicas e historial laboral, etc. Es por tanto que necesitamos "valorar" que tan importante y en donde se localiza dicha información. La información con un valor inestimable para una organización puede tener un pequeño o no valor para otra organización.

- *¿Qué tan vulnerable es la información?*

  Alguna información puede ser muy importante para alguien y puede carecer de interés para alguien mas (por ejemplo una novela de un escritor). Otra información puede ser de gran interés pero puede ser tan

inaccesible, que controles adicionales de seguridad no se justifican (información militar clasificada que está encriptada y almacenada en una computadora ampliamente resguardada con sólo usuario autorizado y sin conexiones de red, es en ejemplo de esto).

Cada uno deberá preocuparse entonces por amenazas físicas (por ejemplo un incendio o un apagón) y accidentes causados por descuido o negligencia de los empleados. Detrás de estos peligros obvios se tendrá que evaluar de manera realista cuantos intentos se han hecho, o podrían ser, para accesar el sistema de manera ilegal o cual sería el impacto de que esto sucediera en el futuro. Si se es el responsable de la información de la Defensa Nacional se deberá preocupar de los departamentos de inteligencia de países extranjeros. Si se está protegiendo los datos del negocio, se deberá estar preocupado por que sus competidores no integren espías dentro de la organización o sobornen a propios empleados a cambio de información. Se deberá recordar también que las amenazas a la información se incrementan conforme el personal aprende más con respecto a las vulnerabilidades del sistema y aquellos métodos de explotación de las vulnerabilidades sean más baratas y fáciles.

- *¿Cuál es el costo de la pérdida o al comprometer la información?*

  Como existen muchos tipos diferentes de costos de seguridad en la información, también hay variedad en las consecuencias. Si hablamos acerca de la pérdida de información vital de la Defensa Nacional, el costo pudiera ser un cataclismo. Si un experimento médico es divulgado o los registros de un paciente son extraviados o comprometidos, la gente puede morir. Si la seguridad de un Cajero Automático es violada, el banco puede perder mucho dinero y, cuando la noticia sea divulgada por los noticiarios, el banco puede sufrir pérdida de confianza de sus clientes y posiblemente problemas legales en contra de los accionistas.

  ¿Y que hay acerca de información estratégica corporativa?, ¿Información de salud o financiera?, cada una de ellas tiene su propio riesgo, costos y consecuencias tanto tangibles como intangibles.

- *¿Cuál es el costo de proteger la información?*

  Es cierto que se deberá incurrir en costos básicos: Se deberán respaldar los datos. No importa que tipo de violación de seguridad ocurra, un desastre natural, un error de usuario o una interrupción; si se tiene un respaldo reciente de los datos se podrá continuar con el servicio.

Hay una gran variedad de costos adicionales. ¿Es necesario comprar un nuevo equipo?, ¿El uso de un producto de seguridad afectará mis tiempos de respuesta del equipo así como su nivel de rendimiento (performance)?, ¿Los controles de seguridad darán la impresión de ser trámites burocráticos a un sistema que se promociona como fácil de uso?.

Aquí también se deberán considerar los diferentes tipos de costos dentro de la organización y evaluar el impacto del costo de la seguridad en relación a los beneficios esperados de seguridad. Una regla es que el costo de la seguridad en la información no deberá exceder el costo financiero y administrativo para la recuperación de esa información (aunque ciertos tipos de información, como aquella de la Defensa Nacional no necesariamente deberá incurrir en esta regla). También es difícil cuantificar el daño realizado por publicidad y por la pérdida de confianza de los clientes. Los controles que son más caros que la información que protegen no son efectivos; la seguridad absoluta se logra a un costo ilimitado.

En base a las respuesta de éstas preguntas, se deberá tomar una determinación, balancear el valor de los activos de información contra los riesgos de pérdidas y los costos financieros y humanos de proteger dicha información. Entonces se tendrá que decidir cuales son las prioridades y que tipos de seguridad (física, sistemas operativos, líneas de comunicaciones, encripción, dispositivos biométricos, etc.) protegen de la mejor manera la información y el presupuesto a además minimizan los riesgos.

En este capitulo se presentarán algunas metodologías cualitativas y cuantitativas que podrán ser aplicadas dentro de la Organización para la elaboración de un análisis y administración de riesgos y así llegar al equilibrio entre valor de las medidas de seguridad y el valor del activo informático a proteger.

A continuación se explicará el modelo del proceso para la Administración de Riesgos que en general deberá ser utilizado por las organizaciones interesadas de conocer cuales son los activos más valiosos, en términos de información, que deberán proteger y en evaluar sus niveles de seguridad sobre los mismos.

MODELO DEL PROCESO DE ADMINISTRACIÓN DE RIESGOS
(Risk Management)

Definimos la administración de riesgos como un proceso sistemático de análisis del medio ambiente (activos, amenazas, riesgos, vulnerabilidades y controles) para ayudar a la gerencia en el proceso de control de pérdidas. El análisis de riesgos lo definimos como una herramienta empleada en el proceso de administración de riesgos para producir una medición del riesgo o de la pérdida esperada.

Otra definición del término administración de riesgos (risk management) es utilizado para describir el conjunto de ideas, modelos, abstracciones, métodos y técnicas que se emplean para controlar el riesgo.

En términos generales existen cuatro alternativas para el control y administración de los riesgos:

1.- EVITAR EL RIESGO:

La evasión del riesgo elimina el evento deshaciéndose de la situación o actividad peligrosa. Si una situación involucra un alto riesgo con un mínimo valor a la organización, se deberá considerar la eliminación del mismo. Cuando se evalúen programas y actividades, considérense fuertemente las actividades que incluyen un alto grado de riesgo a la organización. Por ejemplo, una compañía implementó fines de semana para sus empleados en diversos campamentos como parte de su programa de convivencia pero la compañía aseguradora no pudo asegurar a los empleados debido a que no se contaban con planes de seguros de campamento, así que se tuvieron que eliminar los campamentos para evitar los riesgos asociados.

2.- TRANSFERENCIA DEL RIESGO:

Una definición común de "administración del riesgo" es transferir el riesgo a alguien más, usualmente obteniendo una póliza de seguro. Los convenios y otros contratos son otras alternativas para que el riesgo sea transferido de una parte a otra.

3.- ACEPTACIÓN DEL RIESGO:

La aceptación del riesgo significa que la organización conoce y mantiene el riesgo latente y aún así acepta la responsabilidad de que algunas pérdidas pueden presentarse. Los riesgos no evitados o transferidos se asumen. La aceptación del riesgo es generalmente considerado como "vida peligrosa", pero algunas situaciones y actividades no pueden ser eliminadas o comercialmente aseguradas. Por ejemplo, si un grupo de

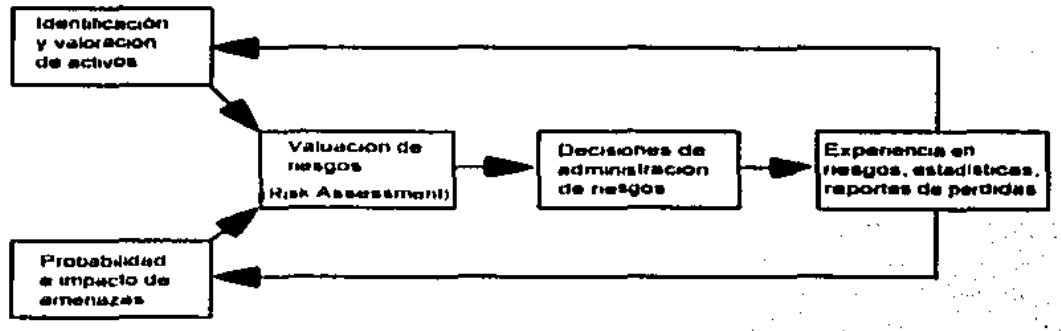
jóvenes decide acampar a las orillas de la ciudad, conociendo el peligro potencial, se asume el riesgo. El auto-seguro "self-insurance" cae dentro de la categoría de aceptación del riesgo.

4.- REDUCCIÓN DEL RIESGO:

La reducción del riesgo debe ser el objetivo de un programa de administración de riesgos. La reducción del riesgo significa reducción de pérdidas. De una u otra manera la reducción del riesgo se da formulando cuidadosamente un grupo de políticas y procedimientos para la organización, así como los estándares para que el mejoramiento pueda ser medido y mejorado.

El análisis de riesgos es a la administración de riesgos, lo que el cálculo al ingeniero. Un administrador de riesgos utiliza el análisis de riesgos para resolver problemas, de esta manera, el análisis de riesgos es visto como el cálculo de la administración de riesgos.

La siguiente figura representa el modelo que describe al proceso de administración de riesgos: se trata de un ciclo de retroalimentación con cinco elementos. Los dos de la izquierda son elementos de entrada, esto es, deben identificarse los activos y asignárseles un valor; las amenazas deben señalarse, así como estimar su probabilidad de ocurrencia e impacto. Dadas estas entradas, procede la valuación de riesgos, a través de la estimación de la probabilidad de que los activos estén sujetos a las amenazas. Esta valuación proporciona material crudo para la toma de decisiones sobre riesgos. Los resultados de estas decisiones, con el tiempo, proporcionan experiencia en riesgos. La experiencia se puede obtener también de otras organizaciones. Los reportes de pérdidas resumen esta experiencia y retroalimentan para perfeccionar la estimación de probabilidad e impacto de amenazas y la identificación y valoración de activos. Así, el modelo se convierte en *iterativo*. El proceso debe repetirse cuando esté disponible nueva información o cuando cambie el medio ambiente.



Entradas:

• *Identificación y valoración de activos:* Como primer paso, debe estudiarse el medio ambiente para identificar los recursos (unidades de procesamiento central, unidades de cinta, unidades de disco, etc.), los recursos dependientes (el buen nombre de la Organización, la capacidad de procesar aplicaciones, programas, etc.) y los recursos controlados (información). Enseguida, se debe asignar un valor para cada activo; la medida estándar es la monetaria. Utilizar como punto de partida "checklists" basados en inventarios de equipo, archivos, programas y otros activos importantes. Preguntar al grupo apropiado de gerentes (provistos con "checklists" e inventarios) para obtener una relación completa de activos. La valoración en ocasiones es más compleja. El valor de algunos elementos es independiente del tiempo, el de otros cambiará. Por ejemplo, las pérdidas pueden variar significativamente dependiendo de si la corriente eléctrica no está disponible por 1, 8, 24 ó 48 horas, o si falla en un momento determinado, como en el cierre de fin de año.

Los elementos no tangibles requieren de mayor reflexión y de un análisis más cuidadoso. Para valuar el nivel concerniente a un delito de cómputo y su publicidad negativa, por ejemplo, un gerente puede contestar a la pregunta, "¿Preferiría tener una pérdida de 10,000 u.s. o ser nombrado por un *delito de cómputo de 3,000 u.s.* en el Wall Street Journal?". Los activos no tangibles por lo general pueden ser valuados estimando cuánto costaría restablecer la situación a la condición previa a la pérdida o estimando el valor del activo para un competidor.

• *Probabilidad e impacto de amenazas:* Significa determinar con qué frecuencia ocurrirá una pérdida y qué efecto tendrá en la Organización. Por lo general, es difícil conseguir información completa a este respecto;

puede bastar entonces un estimado intuitivo, o el manejo de rangos de valores ("la probabilidad de que ocurra el evento está entre 0.25 y 0.60") o la comparacion entre diferentes eventos ("la frecuencia del evento A será dos veces la del evento B"). La precisión y significado de ambos tipos de información puede variar considerablemente. En el mundo real, la información precisa y cuantificable por lo general no existe. En estos casos lo único que puede intentarse es mejorar y utilizar cuidadosamente información cruda.

El ciclo de retroalimentación mostrado en el modelo es una forma excelente de mejorar la calidad de la información. Los reportes de control de pérdidas pueden resultar invaluables.

Otra técnica muy útil es recurrir a los propietarios de los activos para recopilar o desarrollar la información. Los propietarios dependen de la precisión y disponibilidad de la información y de las aplicaciones y tienen que vivir con decisiones basadas en la información.

Otro medio para mejorar la calidad en la información de entrada es emplear un equipo para investigación y acopio. El emplear individuos de diversas áreas funcionales puede dar un balance muy positivo, amplia experiencia y control de calidad.

- *Valuación de riesgos (Risk Assessment):* La valuación de riesgos es la parte medular del proceso de administración de riesgos. Combina la información de entrada sobre activos y amenazas y produce una medición del riesgo o de la pérdida esperada. El resultado es empleado para tomar decisiones de riesgos.

La información de entrada puede ser combinada en diversas formas, cuantitativas y cualitativas. La tendencia en la obtención de la información, ha sido ir de acercamientos muy informales, intuitivos y cualitativos a acercamientos altamente estructurados, formales y cuantitativos. Algunos expertos en la materia creen que la dirección ahora es en el sentido opuesto, por las razones siguientes. Los acercamientos cualitativos tienden a ser relativamente rápidos pero propensos a errores y parcialidad. En el análisis, por lo general, se pasan por alto activos y amenazas y la medición resultante no puede ser defendida o utilizada por otros. En el otro extremo del espectro se encuentra una aproximación conceptual muy atractiva -pura, limpia, matemáticamente correcta, simple en concepto y promete un resultado cuantitativo. Las dos entradas son representadas como:

A = monto ($) de la pérdida resultante de la ocurrencia de la amenaza

P = probabilidad (por año) de la ocurrencia del evento de pérdida

El producto de ambas entradas, L = P x A, es igual a la pérdida esperada (pérdida por cada activo). Esto es, la Organización puede esperar, en promedio, sufrir una pérdida del activo en cuestión de L ($) en un año dado, teniendo la amenaza en cuestión. Lo lógico es calcular la pérdida total esperada (T), la suma de todas las pérdidas sobre los *n* activos y *m* amenazas:

$$\sum_{i=1}^{n} \sum_{j=1}^{m} (P_{ij} \times A_i) = \sum_{i=1}^{n} L_i = T$$

Esta medida (ya sea para un par activo/amenaza o para la pérdida total esperada) puede entonces ser utilizada con información derivada separadamente sobre el costo de los controles y del grado en que éstos reducen la probabilidad de pérdida, para tomar decisiones de seguridad y control. Si un control cuesta menos que la reducción del monto de la pérdida esperada, entonces compra el control; de lo contrario, busca otro.

En resúmen, otra forma de visualizar lo que es la valuación cuantitativa de riesgos es la siguiente:

Los dos *factores principales* en el análisis de riesgos son:

1. *Impacto* (qué tan adverso sería el efecto de una dificultad si ésta se presentara)

2. *Probabilidad* de que esa dificultad se presente en un período específico de tiempo.

Existe una marcada tendencia a valuar el impacto y la probabilidad con más exactitud que la requerida en realidad. Esto contribuye materialmente al tiempo requerido para llevar a cabo la valuación de riesgos, sin obtener el incremento correspondiente en el valor del producto.

Es mejor hacer la valuación de riesgos a través de amplios estimados, tanto del impacto como de la probabilidad. Posteriormente puede trabajarse en refinar ciertos aspectos, si se determina que se requiere mayor precisión para tomar una decisión. Por esta razón, se propone una herramienta para inducir al equipo de análisis de riesgos a ser lo suficientemente inexactos, al menos en la pasada inicial, para completar el trabajo en un tiempo razonable.

Problemas prácticos:

En teoría, esta aproximación matemática es muy simple y directa; sin embargo, en la práctica no es así. Primero, no siempre es posible conseguir la información de entrada en términos monetarios ($) y de eventos por año. Segundo, el tratar con todos los activos y todas las amenazas es frecuentemente un problema demasiado grande. Se requiere una relación de cada pieza de hardware y cada conjunto de información para obtener una imagen verdadera del total de la pérdida esperada, esto resulta demasiado costoso. Más aún, el resultado obtenido no es tan preciso como se requiere. La calidad de los resultados depende directamente de la calidad de las entradas. Finalmente, la información de probabilidad, por naturaleza, está basada en información incompleta, por lo que los valores son inexactos o "suaves". El problema final es humano: la mayoría de la gente tiene problemas al basar decisiones importantes de seguridad y control, en información y probabilidades incompletas.

Soluciones a los problemas prácticos:

Aún cuando la valuación formal de riesgos tiene muchos problemas, puede ser de utilidad. A continuación se sugieren algunos lineamientos:

1. No tratar de incluir todo; dimensionar el alcance a un tamaño manejable y de costo-eficiencia. Enfocarse en los mayores elementos de control de pérdidas, tal vez unos cuantos al mismo tiempo con diferentes esfuerzos.
2. Asegurarse de que los propietarios proporcionen la información de entrada; ellos tienen la mejor información y tienen que vivir con los resultados.
3. Utilizar un equipo para recolectar y analizar la información. El proceso de análisis de riesgos requiere más que el simple acopio de información y su acomodo en una ecuación. La información debe desarrollarse y refinarse; entre más experiencia y profundidad se dé a este esfuerzo, más útil será la información.
4. Recordar que el proceso de análisis por sí mismo es tan importante -o tal vez más- que los resultados.
5. Incluir algún análisis sensitivo; esto es, considerar cuán crítica es la entrada para la salida. Si un ligero cambio en el valor de entrada origina un cambio drástico en la salida, podemos encontrarnos en terreno peligroso.
6. Durante la fase de entrada, registrar porqué y cómo fueron determinados los valores. Tales notas son útiles para mantener la consistencia, credibilidad y para ayudar, a quien va a tomar la decisión, a interpretar la

salida. Además de la información "cruda", obtener información narrativa de soporte, si es posible. Registrar los factores clave para la determinación de valores para la pérdida de activos y la probabilidad de los eventos. Poner las notas en un formato y turnarlos a quienes toman decisiones.

Salida:

La salida de la valuación de riesgos debe mostrarse en una forma fácilmente utilizable por quienes toman las decisiones, en términos de que pueda ser comparada contra el costo de los controles. El formato ideal es la unidad monetaria en una base anualizada. Debido a que la información de entrada carece de precisión y refleja variación en las probabilidades, es importante incluir información sobre la sensitividad de los resultados. Tambien debe adjuntarse la información intermedia y de soporte empleada para obtener los resultados finales.

Retroalimentación:

La retroalimentación en el proceso de valuación de riesgos es crítica para mejorar la precisión y utilidad de la información. Pocas organizaciones han establecido mecanismos formales para facilitar la retroalimentación. No existe coordinación en los esfuerzos para identificar, monitorear y reportar la información, lo que da como resultado que sólo en algunas ocasiones dicha información llegue a la gente adecuada. Un sistema de reporte de pérdidas proporciona un excelente mecanismo de retroalimentación. Deben definirse bien los tipos de pérdidas y establecer los lineamientos para el reporte periódico y excepcional de incidentes. La retroalimentación debería venir no sólo de las funciones normales de control como seguridad, auditoría, administración de riesgos, seguros, sino también de los departamentos de usuarios y del personal de control de calidad. Los factores importantes son: quién es el primero en enterarse de las pérdidas, quién es el afectado por las pérdidas y quién es el responsable de corregir las situaciones de pérdida.

Hasta este punto se ha descrito el proceso de administración de riesgos de manera genérica, se recomienda, como anteriormente se mencionó, que para realizar un análisis de riesgos de manera cuantitativa se deberá contar con apoyo de software específico para tales efectos y una fuerte base de información estadística.

A continuación se presentarán una serie de cuestionarios recomendados por diferentes autores, para utilizarlos como apoyo para la recopilación de información así como para la identificación y valoración de activos informáticos.

ESTUDIO DE SEGURIDAD

PANORAMA GENERAL PARA LA EVALUACIÓN DE PERDIDAS POR APLICACIONES

El propósito del presente cuestionario es el de concientizar del impacto o pérdida potencial de su aplicación al no contar con ella.

INSTRUCCIONES: *Invierta no más de una hora para responder este cuestionario. Responda únicamente aquellas preguntas de las cuales tiene el conocimiento directo o pueda aproximar razonablemente su respuesta.*

1.- Proporcione el nombre del ejecutivo que tiene el mayor conocimiento acerca del valor, beneficios y controles de la aplicación.

NOMBRE APELLIDO DEPARTAMENTO TELEFONO/EXTENSIÓN

2.- Encierre en un circulo la frecuencia con que se corren los jobs de la aplicación:

a) No tiene jobs b) Diariamente c) Semanalmente d) Mensualmentee) Trimestralmente f) Anualmente

g) A solicitud h) En línea, Sólo lectura i) En línea j)Otra _____

3.- ¿Cuál es número aproximado de transacciones procesadas por ciclo? _____

4.- ¿Cuál es el costo mensual del equipo aproximado para la aplicación?

5.- ¿Cuál es el número de módulos de la aplicación? _____ y promedio de líneas de código por modulo? _____

6.- ¿Cuál es el número de personal que da mantenimiento a la aplicación? _____

7.- ¿Cuál es el número de gente que depende de la aplicación? _____

8.- ¿El plan de recuperación o de contingencias incluye todos los elementos para recuperar la aplicación y sus componentes desde un almacenamiento externo (incluyendo programas, datos, utilerías)? SI _____ NO _____

Ultimo día probado _____

En el caso de que no, estime el costo máximo de recuperación de los elementos necesarios para que la aplicación funcione, asumiendo que todas las copias del centro de cómputo se destruyeron. Dólares _____, Días en recuperar _____.

9.- Si la aplicación no tiene un control de cambios, estime el máximo costo asociado con la completa recuperación de los componentes de la aplicación (programas, procedimientos, JCL's, etc.), considerando que toda la lista de software fue destruida del centro de cómputo (costo y tiempo para remplazar el sistema a un estatus operativo).

Dólares _____, Días en recuperar _____.

10.- Dependencia de utilerías. Identifique las utilerías requeridas para que la aplicación procese correctamente.

Utilerías del Sistema:

a.-_____ b.- _____ c.- _____ d.- _____ e.- _____ f.- _____

g.-_____ h.-_____ y.-_____ j.- _____ k.-_____ l.- _____

Utilerías de Datos:

a.-_____ b.- _____ c.- _____ d.- _____ e.- _____ f.- _____

g.-_____ h.-_____ y.- _____ j.- _____ k.-_____ l.- _____

11.- Dependencia de Hardware. Indique los requerimientos de hardware para el procesamiento correcto de la aplicación. Identifique CPU's, controladores de almacenamiento, dispositivos de almacenamiento, líneas telefónicas y velocidades, terminales, plotters, y otros (indique proveedor, modelo y cantidad).

a.-_____ b.- _____ c.- _____ d.- _____ e.- _____ f.- _____

g.-_____ h.-_____ y.- _____ j.- _____ k.-_____ l.- _____

12.- ¿La aplicación requiere de formas preimpresas que deberán estar disponibles para que la aplicación procese adecuadamente?

SI_____ NO _____ Número de formas especiales o preimpresas _____ Numero de semanas que cubre el almacén _____

13.- Liste por orden de importancia, los nombres de los programas que deberán ser ejecutados para que la aplicación se procese satisfactoriamente.

Nombre de programas Superiores	Nombre de programas Inferiores
_____, _____, _____	_____, _____, _____
_____, _____, _____	_____, _____, _____
_____, _____, _____	_____, _____, _____

14.- ¿Existe alguna persona crucial para la aplicación la cual pueda o su departamento, causar problemas considerables en el mantenimiento o producción de la aplicación? Si existe, estime el numero de días que tomará orientar el remplazo de responsabilidades y habilidades para el mantenimiento de la aplicación. SI _____ NO _____ Numero de días _____ Nivel de Conocimiento/Estudios _____

15.- Consideración de acceso público a datos sensitivos:

a. ¿La aplicación permite acceso o produce datos dirigidos al público, por ejemplo: público en general, clientes, agencias, proveedores, etc.?

SI _____ NO _____

b. Si la respuesta es afirmativa: ¿Cuál es el número de personas que tienen acceso?

e. ¿Son los datos de la aplicación especialmente sensitivos? En otras palabras, ¿Contiene información que es personal como situación de salud, registros personales, cuentas de inversión, etc?

SI _____ NO _____

16.- ¿La aplicación proporciona información ideal para hacer mal uso de la misma? En otras palabras, ¿La aplicación incluye información de cuentas por pagar, cuentas por cobrar, cheques, flujo de caja, equipos, etc.?

SI _____ NO _____ ¿Cual? _____ Si la respuesta es afirmativa, ¿Cual es el valor de los activos que controla la aplicación? $_____

17.- ¿Si la aplicación llegara a ser completamente inoperable, cuál sería el impacto en dólares? Considere niveles de servicio, personal ocioso, flujo de caja de cuentas por pagar y por cobrar, penalizaciones gubernamentales, etc.

	Actual	Acumulado		Actual	Acumulado
1 Hora	$_____	$_____	4 Días	$_____	$_____
2 Horas	$_____	$_____	8 Días	$_____	$_____
4 Horas	$_____	$_____	16 Días	$_____	$_____
8 Horas	$_____	$_____	1 Mes	$_____	$_____
16 Horas	$_____	$_____	2 Mese	$_____	$_____
1 Día	$_____	$_____	3 Meses	$_____	$_____
2 Días	$_____	$_____	6 Meses	$_____	$_____

ESTUDIO DE SEGURIDAD

INVENTARIO DE APLICACIONES

Administrador de Proyecto: _____ Fecha: _____

Responsable de la Aplicación: _____

Nombre de Aplicación: _____

1.- Estatus del desarrollo de la aplicación: Porcentaje de la aplicación en producción: _____%

2.- Mencione a los usuarios que tienen el mayor conocimiento acerca del valor, beneficios y controles de la aplicación

NOMBRE	PATERNO	DEPARTAMENTO	TELÉFONO	PUESTO

3.- Encierre en un circulo la frecuencia de ejecución de la aplicación:

a) No tiene jobs b) Diariamente c) Semanalmente d) Mensualmente e) Trimestralmente f) Anualmente

g) A solicitud h) En línea, Sólo lectura i) En línea j)Otra _____

4.- ¿Cuál es número aproximado de transacciones procesadas por ciclo? _____

5.- ¿Cuál es el costo mensual aproximado reportado como Reportes de utilización de equipo (Machine Utilization Reports MUR)? _____

6.- Indique cual sistema es utilizado en su aplicación:

	Data Entry	Main Processor	Remote Job Entry
IBM			
CASE			
HP			
UNISYS			
Burroghs			
Tandem			
Otro			

7.- ¿Cuál es el número de módulos de la aplicación en producción? _____ ¿Cuál es el promedio de líneas de código? _____

8.- ¿Cuál es el número de personal de sistemas que proporciona mantenimiento a la aplicación?

_____

9.- ¿Cuál es el número promedio mensual de errores de programación? _____

10.- ¿Cuál es el promedio de tiempo de corrección de programas? _____

11.- ¿El plan de recuperación o de contingencias incluye todos los elementos para recuperar la aplicación y sus componentes desde un almacenamiento externo (incluyendo programas, datos, utilerías)? SI _____ NO _____ Ultimo día probado _____

En el caso de que no, estime el costo máximo de recuperación de los elementos necesarios para que la aplicación funcione, asumiendo que todas las copias del centro de cómputo se destruyeron. Dólares _____. Días en recuperar _____.

12.- Si la aplicación no tiene un control de cambios, estime el máximo costo asociado con la completa recuperación de los componentes de la aplicación (programas, procedimientos, JCL's, etc.), considerando que toda la lista de software fue destruida del centro de cómputo (costo y tiempo para remplazar el sistema a un estatus operativo).

Dólares $_____. Días en recuperar _____.

13.- Dependencia de utilerías. Identifique las utilerías requeridas para que la aplicación procese correctamente.

Utilerías del Sistema:

a.- _____ b.- _____ c.- _____ d.- _____ e.- _____ f.- _____

g.- _____ h.- _____ y.- _____ j.- _____ k.- _____ l.- _____

Utilerías de Datos:

a.- _____ b.- _____ c.- _____ d.- _____ e.- _____ f.- _____

g.- _____ h.- _____ y.- _____ j.- _____ k.- _____ l.- _____

14.- Dependencia de Hardware. Indique los requerimientos de hardware para el procesamiento correcto de la aplicación. Identifique CPU's, controladores de almacenamiento, dispositivos de almacenamiento, líneas telefónicas y velocidades, terminales, plotters, y otros (indique proveedor, modelo y cantidad).

a.- _____ b.- _____ c.- _____ d.- _____ e.- _____ f.- _____

g.- _____ h.- _____ y.- _____ j.- _____ k.- _____ l.- _____

15.- ¿La aplicación requiere de formas preimpresas que deberán estar disponibles para que la aplicación procese adecuadamente?

SI _____ NO _____ Número de formas especiales o preimpresas _____

16.- Liste el nombre de los programas necesarios para que la aplicación se procese satisfactoriamente.

Nombre de programas

_____, _____,

_____

_____, _____,

_____

_____, _____,

_____

17.- ¿Existe alguna persona crucial para la aplicación la cual pueda o su departamento, causar problemas considerables en el mantenimiento o producción de la aplicación? Si existe, estime el número de días que tomará orientar el remplazo de responsabilidades y habilidades para el mantenimiento de la aplicación. SI _____ NO _____ Número de días _____ Nivel de Conocimiento/Estudios _____

18.- Consideración de acceso público a datos sensitivos:

a. ¿La aplicación permite acceso o produce datos dirigidos al público, por ejemplo; público en general, clientes, agencias, proveedores, etc.?

SI _____ NO _____

b. Si la respuesta es afirmativa: ¿Cual es el número de personas que tienen acceso?

c. ¿Son los datos de la aplicación especialmente sensitivos? En otras palabras, ¿Contiene información que es personal como situación de salud, registros personales, cuentas de inversión, etc?

SI _____ NO _____

19.- ¿La aplicación proporciona información ideal para hacer mal uso de la misma? En otras palabras, ¿La aplicación incluye información de cuentas por pagar, cuentas por cobrar, cheques, flujo de caja, equipos, etc.?

SI _____ NO _____ ¿Cuál? _____ Si la respuesta es afirmativa, ¿Cuál es el valor de los activos que controla la aplicación? $_____

20.- Por cada tipo o clasificación de datos, marque con "X" aquel medio de almacenamiento requerido para almacenar la información.

	A CLIENTES	B PROVEEDORES	C POLITICAS	D TRANSACCIONES	E FLUJO/AVANCES	F CONTABILIDAD	G PRESUPUESTO	H PERSONAL	I DATOS EDP	J PRODUCTOS	K MISCELANEOS	L MISCELANEOS	
1													DASD
2													TAPE
3													MASS STORAGE
4													MICROFILM/FICHE
5													C A DISK
6													IV PHASE DISK
7													HP 3000
8													FLOPPY DISK
9													LASER DISK
10													OPTICAL DISK

El siguiente cuestionario junto con una interpretación adecuada, permitirá establecer un marco de recomendaciones relacionadas a la protección de sistemas de cómputo contra ataques de virus. El cuestionario está diseñado para valuar los niveles de vulnerabilidad del sistema contra virus (preguntas 1 a 18) y para determinar el grado de impacto que esta contaminación pudiera tener en la compañía (preguntas 19 a 29).

El cuestionario deberá ser contestado por tres o seis empleados con nivel de subgerencia o gerencial, de cuatro a ocho personas de sistemas y algunos usuarios de los sistemas escogidos al azar. Las diferencias en las respuestas deberán ser aclaradas con los participantes para que únicamente un set de respuestas sea sujeta al análisis en el esfuerzo de valorización.

Cada pregunta tiene asignado un peso relativo conforme a su importancia en la determinación del nivel de vulnerabilidad/impacto. Las respuestas a cada pregunta también tienen un peso, el valor de 1 representa el nivel más bajo de riesgo y el 4 el más alto nivel. Algunas de las preguntas podrán parecer subjetivas y por lo tanto no afectarán el resultado, estas preguntas han sido desarrolladas para proporcionar mayor información si es necesario.

Entre más alto el marcador, más alto será el grado de vulnerabilidad/impacto, la tabla 1 puede ser utilizada como una guía para determinar la posición aproximada del grado de exposición del sistema de cómputo.

1.- ¿Su sistema de cómputo está en un ambiente cerrado o puede ser accesado remotamente?(5)
A. Cerrado ____ (1) B. Accesado remotamente ____ (4)

2.- ¿Su sistema está en red con otras computadoras?(5)
A. Si ____ (4) B. No ____ (1)

3.- ¿Si la pregunta 2 fue SI, son esas computadoras parte de su organización?(4)
A. Si ____ (1) B. No ____ (4)

4.- Si su equipo puede ser accesado remotamente, ¿que mecanismo de acceso se utiliza?(5)
A. Dial-in (marcado) ____ (4) B. Conexión directa (Leased line point-to-point) ____ (2)

5.- ¿Pueden medios de almacenamiento (disquetes, cintas) de fuentes externas, ser introducidas a su sistema?(5)
A. Si ____ (4) B. No ____ (1)

6.- ¿Esta restringido el acceso a información confidencial?(4)
A. Si ____ (1) B. No ____ (4)
Si la respuesta es afirmativa, explique como se restringe el acceso:

7.- ¿Qué sistema operativo está instalado en su computadora?

8.- ¿La organización utiliza software desarrollado por algún proveedor o se desarrolla en casa?(5)
A. Desarrollos de proveedor (4)
B. Desarrollos en casa (2)
C. Ambos (1)

9.- Si el software es adquirido de diferentes proveedores, ¿existe algún programa implementado de aseguramiento de calidad para la detección de virus?(5)

A. Si _____ (2) B. No _____ (4)

10.- ¿El sistema incluye algún mecanismo de seguridad que asigne identificadores de usuario (users-id) y que solicite password para cada usuario?(5)

A. Si _____ (1) B. No _____ (4)

11.- ¿El sistema registra todos los passwords?(4)

A. Si _____ (1) B. No _____ (4)

12.- ¿El sistema registra todas las fallas al tratar de firmarse (log on)?(4)

A. Si _____ (1) B. No _____ (4)

13.- ¿El equipo tiene algún producto para la detección prevención de virus?(5)

A. Si _____ (1) B. No _____ (4)

Si la respuesta es afirmativa, ¿que productos utiliza?

14.- ¿Ha sido alguno de los sistemas contaminado con virus anteriormente?(5)

A. Si _____ (4) B. No _____ (1)

15.- Si la respuesta anterior es afirmativa, ¿Cuánto tiempo permaneció el virus antes de que fuera detectado?(5)

A. Un día o menos (1)
B. Entre un día y una semana (2)
C. Entre una semana y un mes (3)
D. Más de un mes (4)

16.- ¿Cómo detectó el virus?

17.- ¿Cuál fue el valor monetario del daño producido por el virus?(5)

A. Menos de $1000 (1)
B. Entre $1000 y $5000 (2)
C. Entre $5000 y $10000 (3)
D. Más de $10000 (4)

18.- Con las características actuales del antivirus instalado, ¿Cuál de esas estuvieron presentes cuando el virus invadió el sistema?

Explique:

19.- ¿Cuánto dinero, si aplica, se destina del presupuesto para educación e investigación acerca de las nuevas formas de los virus computacionales?(4)

A. 0% (4)
B. 10% (3)
C. 20% (2)
D. Más de 20% (1)

20.- ¿Cuál es el impacto de una hora de caída de sistema en su organización?(5)

A. Interrupción del servicio, caída de la planta, grupos staff ociosos..........(3)
B. Inconveniencia pero las actividades del centro del negocio continúa (2)
C. No impactó en la interrupción de las actividades del negocio (1)

21.- ¿Cuál es el impacto de una caída de sistema total?(5)

A. Desastroso, no existe una fuente de respaldo..........(4)
B. Se requiere de una mayor visión externa (3)
C. Caro, los procesos primordiales pueden conservarse con algún costo extra y con reducidos niveles de calidad (2)
D. Mínimo, existen procedimientos adecuados de respaldo (1)

22.- ¿Cuál es el porcentaje del costo del área de Seguridad Informática con respecto al costo total de la organización?(5)

A. Más del 10% (3)
B. Del 2% al 10% (2)

C. Menos del 2% (1)

23.- Número de sistemas:(5)

A. # sistemas en línea (4)

B. # sistemas en batch (2)

(NOTA: Para valorar respuestas, adicione (1) para cada sistema batch adicional y (2) para cada sistema en línea adicional.

24.- Facilidad de recuperación después de una falla de seis horas:(5)

A. De 3 a 4 días (4)

B. De 12 a 24 horas (3)

C. de 1 a 12 horas (2)

D.- Casi instantáneo (1)

25.- Recuperación después de una falla de control de calidad:(5)

A.- Tiempo de consumo, caro, muchos sistemas interrelacionados (3)

B.- Alguna interrupción y gasto (2)

C.- Relativamente rápido, daño bien controlado (1)

26.- Factibilidad de copiado manual:(5)

A.- Imposible (3)

B.- Algunas cosas posibles (2)

C.- Relativamente sencillo (1)

27.- ¿Cuenta con procedimientos especiales de respaldo para protección contra daño por virus o contra daño incurrido por otras interferencias o interrupciones?(4)

A.- Si (1) B.- No (2)

Si contesto que si, explique_____

28.- En caso de interrupcion del sistema, ¿Cual es la pérdida asociada por una hora de interrupción?(5)

A.- Menos de $1000 u.s (1)

B.- Entre $1000 y $5000 u.s.....(2)

C.- Entre $5000 y $10 000 u.s.....(3)

D.- Más de $10 000 u.s.....(4)

Si la respuesta es D, proporcione el monto aproximado de la pérdida:_____

29.- En caso de interrupción del sistema, ¿Cual es la pérdida asociada por un día de interrupción?(5)

A.- Menos de $1000u.s (1)

B.- Entre $1000 y $5000 u.s.....(2)

C.- Entre $5000 y $20 000 u.s.....(3)

D.- Más de $20 000 u.s.....(4)

Si la respuesta es D, proporcione el monto aproximado de la pérdida:_____

30.- En caso de interrupcion del sistema, ¿Cual es la pérdida asociada por una semana de interrupción?(5)

A.- Entre $1000 y $5000 u.s.....(1)

B.- Entre $5000 y $10 000 u.s.....(2)

C.- Entre $10 000 y $30 000 u.s.....(3)

D.- Más de $30 000 u.s.....(4)

Si la respuesta es D, proporcione el monto aproximado de la pérdida:_____

TABLA I:

CALIFICACIÓN DEL CUESTIONARIO VULNERABILIDAD/IMPACTO

VARIABLE	RANGO DE PUNTUACIÓN	NIVEL
Vulnerabilidad	140 o menos	Bajo
Vulnerabilidad	141-240	Medio
Vulnerabilidad	241-325	Alto
Impacto	85 o menos	Bajo
Impacto	86-120	Medio
Impacto	121-205	Alto

Como se comentó anteriormente, el nivel de vulnerabilidad de nuestro sistema contra contaminación de virus será estimado sumando los valores de las respuestas a las preguntas 1 a 18; entre más alto sea el número obtenido, será necesario incrementar las medidas de control. De la misma manera al responder las preguntas 19 a 29, el impacto al contaminarse un sistema de cómputo será mayor si la suma de puntos a las respuestas es un marcador mayor; esto también requiere analizar los puntos en donde sean requeridas el incremento de medidas de seguridad.

Otra forma de mantenerse actualizado y consciente de la problemática de seguridad que día a día nos aqueja, es la de investigar continuamente en revistas, artículos, material, etc. especializados tópicos de referencia en la materia; a continuación se presenta una lista de 25 tips para proteger una LAN que se consideran necesarios para mantener un nivel aceptable de seguridad y que con el paso del tiempo deberán ser revisados y actualizados.

25 TIPS PARA PROTEGER SU LAN

1. Cada individuo que desea accesar la red deberá proporcionar un nombre de usuario válido (user-id) y una clave de acceso (password) para poder conceder el acceso.
2. Adicionalmente al user-id/password, se debe implementar un nivel de control extra cuando sea un acceso dial-up a la LAN.
3. La seguridad del sistema operativo de la LAN debe ser implementado y utilizado completamente.
4. Se deben contemplar controles de seguridad dentro de las aplicaciones que corren en redes organizacionales complementando el sistema operativo de la red.
5. El Plan de Recuperación en caso de Desastre (Disaster Recovery Plan DRP) para redes departamentales y la columna vertebral de la organización (si aplica), debe ser desarrollado y probado en conjunto con otros elementos del DRP completo.
6. Ninguna LAN debe estar conectada a la columna vertebral de la organización o a otra red sin la autorización de un grupo de control central.
7. Bajo condiciones normales, sólo al personal operativo se le permite operar los mainframes y sólo a los administradores de la red estarán autorizados para operar los servidores de la red.
8. Los servidores de la red deben estar protegidos en áreas en donde no exista acceso a cualquier personal.
9. La operatividad del equipo de generación de energía eléctrica y baterías de respaldo, debe ser verificada periódicamente para todo tipo de computadoras y equipo de comunicaciones.
10. Cada servidor o estación de trabajo debe estar conectado a un supresor de picos o algún otro dispositivo para este fin, para protegerse contra cargas eléctricas fuera de los rangos.
11. Debe existir un departamento de adquisiciones a través del cual se debe asesorar en la compra de componentes de red por medio del departamento de compras.
12. Las prácticas de mantenimiento en las áreas donde esta el server y las estaciones de trabajo, no deben incrementar el factor de riesgo.

13. Debe existir un procedimiento escrito formal para reportar incumplimientos de seguridad o incidentes sospechosos y para las acciones de seguimiento.
14. Debe existir un procedimiento formal para revisar apagones eléctricos e investigar su incidencia.
15. Debe existir un procedimiento formal para el control de cambios que incluya pruebas de seguridad el cual deberá ser utilizado para administrar todas las modificaciones normales en cualquier software que corra en producción en cualquier plataforma.
16. Debe existir una aplicación para la administración de grupos de trabajo que permita el acceso a usuarios con base en "need-to-know" y definición de privilegios proporcionando el acceso necesario para realizar su trabajo, no más.
17. Los archivos de producción no deberán usarse para pruebas.
18. Los respaldos de sistemas básicos de LAN, deberán generarse periódicamente almacenando una copia dentro del site y otra fuera y además deberan ser probados.
19. Las aplicaciones deben ser revisadas y actualizadas regularmente en función de nuevas tecnologías, cambios del negocio y migración de aplicaciones a LAN´s y otras plataformas downsized[27].
20. Se debe considerar dentro del Plan de Recuperación ante Desastres (DRP), los tiempos de respuesta para conseguir líneas de comunicación, equipo, dispositivos especiales, fuentes de poder ininterrumplibles (UPS), etc., además de la construccion y configuración de la LAN.
21. Aquel personal que tenga su propia computadora en casa y que realice actividades de su trabajo, debe scanear sus disquetes para detectar virus antes de introducirlos en las redes de producción.
22. Los mensajes significativos y transacciones entradas a los sistemas en línea, LANes y E.Mails seriados, y tiempos de uso de sistemas deberán ser registrados y respaldados para futuras auditorias.
23. Los usuarios recién contratados de la red, deben asistir a sesiones de seguridad seguidos de recordatorios periódicos.
24. Remover los identificadores de usuarios obsoletos.
25. El personal de seguridad, de desarrollo y de la red deben trabajar activamente para disminuir la molestia del uso de identificadores por medio de la simplificación de mensajes, minimizando los "log-on" requeridos, coordinando cambios de passwords, etc.

---

[27] Esto sucede cuando las compañías migran de mainframes a ambientes LAN (cliente-servidor).

CONCLUSIONES

Las conclusiones a las que he llegado al elaborar el presente trabajo de tesis son las siguientes:

- Las organizaciones preocupadas por la información que manejan llámese productos, servicios, estrategias, convenios, alianzas estratégicas, fórmulas químicas, secretos industriales, etc., deberán establecer una función dentro de sus organizaciones que se encargue de detectar vulnerabilidades en la protección de la información, establecer programas para una adecuada clasificación de la información y definir los roles y responsabilidades del personal de la organización para el manejo de la misma, definir las medidas de seguridad y controles para la protección de la información en sus diferentes medios de expresión, y establecer programas y sesiones de concientización y difusión de políticas, normas, estándares y controles.
- Es claro que el compromiso deberá involucrar de manera inicial a la alta Dirección de la organización, ya que sin este, cualquier esfuerzo realizado no llegará a concretarse ya que difícilmente se llegará a una disminución de posibles pérdidas económicas y de imagen a consecuencia de la falta de disponibilidad, pérdida de integridad y confidencialidad de la información.
- La responsabilidad de la seguridad dentro de una organización deberá ser compartida: es difícil que únicamente la función de Seguridad Informática llegue a dar resultados sin la ayuda del personal que día con día elabora los diferentes procesos de la información de manera automatizada o manual junto con el apoyo y supervisión de los niveles adecuados dentro de la Organización.
- La manera de evaluar el compromiso de la Dirección de las organizaciones, es observando el apoyo tanto a nivel de recursos humanos asignados como al nivel de capacitación y demás recursos que se asignen a dicho personal. Esto no quiere decir que deberá ser una área con demasiado personal, estará en función del tipo de información manejada, su clasificación y del tamaño de la Organización.
- La Dirección de las organizaciones de manera inicial deberá proporcionar claramente sus políticas y directrices en materia de seguridad en la información, siendo estas, las guías que lleven por el camino adecuado la función de Seguridad Informática.
- La seguridad es un conjunto de procesos que no tienen final; gracias a la tecnología, nuevos procesos y técnicas será necesario revisar continuamente el grado de obsolescencia o aplicabilidad de los controles establecidos.
- La seguridad informática deberá ser vista como una herramienta para evitar pérdidas no como una herramienta para poner trabas en el desarrollo y procesamiento de la información; es aquí el gran reto al que se deberá llegar: lograr un equilibrio entre la seguridad y la complicación o burocracia.

En este trabajo de tesis se aportan algunas ideas de la manera en que deberá ser conformada la función de la Seguridad Informática, cómo debe interactuar con las diferentes áreas de la organización que intervienen directa e indirectamente con el proceso automatizado o manual de información.

También se proporcionan elementos como son los controles básicos de seguridad, guías y lo que deberá ser un análisis de riesgos para valorar, verificar y definir las medidas de seguridad actuales y cuales podrían ser implementadas para incrementar los niveles de seguridad de los activos informáticos de la organización.

- Con lo anteriormente expuesto se concluye que el presente trabajo de tesis proporciona los elementos básicos para establecer una función de Seguridad Informática preocupada por la protección de los bienes informáticos de la organización.

El beneficio para la Escuela Nacional de Estudios Profesionales plantel Aragón y en especial a los profesores y estudiantes de la carrera de Ingeniería en Computación es crear la conciencia para que actúen dentro de sus labores diarias, como son la docencia y desempeño profesional, con seguridad; no únicamente en aspectos físicos, sino considerar los aspectos de seguridad en la información, en su manejo, clasificación, implantación de esquemas de verificación y apego a la seguridad, etc. Considero que es necesario que los profesores incluyan tópicos de seguridad en cada una de las materias que así lo requieran para preparar a los estudiantes con un mayor nivel de competitividad y conocimiento en el ámbito profesional.

GLOSARIO DE TÉRMINOS

Administracion de la seguridad	Es el manejo y control de los recursos y atributos de seguridad con el fin de asegurar la proteccion de la informacion.
Algoritmo de encripcion.	Conjunto finito de reglas matematicas para codificar información de manera ilegible por medio de una llave.
Algoritmo DES	Data Encryption Standard (Estandar de Encripcion de Datos), es un estándar basado en series de sustituciones, rotaciones, intercambios y multiplicacion de numeros primos de los bits que componen a la información. Es un algoritmo diseñado y sancionado por el gobierno de USA para la encripción de datos. Encima de la encripción, DES genera una llave única de 64 bits sin la cual la información correspondiente no puede ser traducida a su significado original.
Altamente restringida	Información que requiere del más alto grado de seguridad y de medidas especiales para su protección.
API (Application Program Interface)	Rutinas, programas, interfases desarrolladas para uso común dentro de una diversidad de aplicaciones. Por ejemplo, Windows está dearrollada por una gran variedad de API's. Es un conjunto de llamadas y rutinas formales que pueden ser referenciadas por un programa para accesar los servicios de la red. Es un lenguaje utilizado por una aplicacion para comunicarse con el sistema operativo u otro systema como el DBMS (DataBase Management System). Las APIs son implementadas escribiendo funciones "call" dentro de los programas las cuales proveen la liga a una subrutina especifica para su ejecución.
Aplicación	Conjunto de programas desarrollados para proporcionar soporte y respuestas automatizadas a las areas de la Institución.
Arquitectura	Descripción tecnologica y funcional de los sistemas informáticos definiendo sus componentes, funciones e interrelaciones.
Atributo	Conjunto de elementos y rubros de seguridad considerados para la protección de información.
Auditabilidad (atributo)	Propiedad que tiene un sistema manual o automatizado para rastrear, registrar y generar información de eventos significativos
Autentificación	Consiste en dar validez o legitimidad a un ente autorizado (usuario, oficina, programa, etc.).
Clave de Acceso	Clave confidencial que permite validar la legitimidad del usuario o aplicación portador de la misma (Password).
Código no autorizado	Código residente en un equipo y que no cuenta con la autorización o visto bueno del nivel superior correspondiente.
Confidencial	Característica de la información de ser manejada con discreción, absteniéndose de proporcionarla a personas que no tengan la responsabilidad y facultad para hacer uso de ella dentro o fuera del Grupo, y evitando su acceso a los registros o archivos.
Confidencialidad (atributo)	Atributo de la protección de información que como principal característica limita el acceso y divulgación de información.

Consistencia	Característica que garantiza la coherencia y permanencia de los atributos de seguridad.
Contingencia	Situación que en caso de presentarse puede causar pérdidas de información; o degradación o interrupción del servicio.
Continuidad	Capacidad de los procesos para otorgar servicios y estar disponibles de manera ininterrumpida.
Correspondencia	Capacidad que permite establecer que entre origen y destino, así como entre resultados iniciales y finales de la información , exista congruencia, veracidad y reciprocidad
Criptografía, encripción	Técnica de ocultamiento de información, que convierte códigos legibles a códigos ilegibles.
Custodio	Es un ente (departamento, área o persona) autorizado para la posesión de la información y el cual tiene derecho a proteger, mantener y utilizar controles de uso de la información en un ambiente operativo.
Cuenta	Clave de identificación asignada a usuarios y aplicaciones para acceso y uso de recursos informáticos y de datos.
Datos	Una representación de la información, conocimiento, hechos, conceptos o instrucciones que pueden o son preparados de manera formal para ser almacenados o procesados dentro de una computadora. los datos pueden estar estructurados de cualquier forma, incluyendo pero no limitando, su impresión, almacenamiento magnético u óptico, tarjetas perforadas o simplemente almacenadas dentro de la memoria de la computadora.
DISA (Direct Inward System Access)	Es una característica de algún sistema telefónico que permite que un usuario externo marque directamente al sistema telefónico y accese todas las características y facilidades del mismo. DISA es utilizado típicamente para realizar llamadas de larga distancia desde el hogar utilizando los teléfonos de la compañía debido a que son más baratas las llamadas de este tipo. También son utilizadas para grabar un dictado para que lo mecanografíe el pool secretarial. Con ayuda del DISA se pueden marcar diferentes extensiones sin necesidad de la ayuda (o impedimento) de una operadora.
Disponibilidad (atributo)	Atributo de protección de información que asegura el funcionamiento de tecnología y el otorgamiento de servicio de manera continua y oportuna.
Elemento de seguridad	Cualidad de seguridad establecida para proteger a los datos y los recursos informáticos.
Encripción	Es el método más seguro para la protección de la información; se utiliza una fórmula matemática para mezclar datos almacenados en archivos, para leer la información el usuario debe digitar el código secreto (llave de encripción). La llave de encripción habilita al proceso para desmezclar (desencriptar) la información haciéndola leíble. Sin la llave de encripción la información permanece mezclada e incomprensible.
Encripción "al vuelo"	La encripción "al vuelo" significa que los datos almacenados en el disco son desencriptados solamente en la memoria de la computadora, ahorrando así, tiempo y asegurando la integridad de los datos.
Entes	Acepción otorgada a oficina y usuarios.
Facultad	Derechos otorgados a los entes para accesar y utilizar información.

Firewalls	Es un conjunto de componentes colocados entre dos redes con las siguientes propiedades: Todo el trafico deberá pasar a través del "firewall" (pared de fuego) desde afuera hacia adentro y viceversa. Solamente el trafico autorizado, definido por las políticas de seguridad locales, podrá pasar. El firewall por si mismo, es inmune a la penetración. El uso de estos firewalls, se recomienda para aquellas organizaciones que tienen información sensitiva en su red privada y requieren conexión a redes públicas y para aquellas que deseen limitar el acceso a partes de una red bajo TCP/IP vía Internet. Dentro de las ventajas del uso de firewalls se tiene la de proporcionar seguridad en la conectividad para Internet contra espías industriales, hackers, etc. Proporciona también seguridad interna a los dominios. Proporciona elementos de detección en tiempo real de log-in, pistas de auditoria y detección de intrusos.
Firmware	Microprogramación cableada. Es una categoria de chips en memoria que mantienen su contenido de manera eléctrica en tecnologías ROMs, PROMs, EPROMs y EEPROMs. Firmware llega a ser el "hard software" cuando se conserva un programa de manera no volátil. Software contenido en memoria semipermanente. Firmware se utiliza conjuntamente con hardware y software compartiendo las características de ambos.
Función	Conjunto de actividades asignadas a una persona o conjunto de personas.
Hacker	Conocido en el ambiente también como empleado de cuello blanco, es aquel miembro de la organización que inicialmente era descrito como cualquier persona que invierte mucho tiempo explorando las capacidades de una computadora; actualmente se le conoce como a la persona que aprovechándose de ese conocimiento lo explota para fines de ataque a la organización como por ejemplo lograr acceso a un sistema de cómputo y violar barreras tecnológicas de seguridad.
Identificación	Reconocer que los usuarios o recursos informáticos son iguales a los originalmente descritos.
Implementacion	Diseño.
Implantación	Poner en marcha pasando por la implementación.
Integridad (atributo)	Atributo de la protección de información cuya principal característica es validar lo original, completo y exacto de la información; asegurando que no haya sufrido alteración.
Kerberos	Es un esquema y sistema de seguridad para cliente servidor desarrollado en el MIT que autentifica usuarios. No proporciona autorización a los servicios de las bases de datos, únicamente establece la identidad en la entrada (logon) a lo largo de toda la sesión de trabajo. Es un protocolo de autentificación confiable y tripartita en el cual: a) El usuario o cliente contacta al "server de autentificacion" solicitándole una llave para accesar a un server específico b) El "server de autentificación" responde encriptando la llave c) Esa llave consiste en: Un ticket para el server Una llave de sesión temporal (llave de sesión)

	d) El cliente transmite el ticket (el cual contiene la identidad del cliente y una copia de la llave de sesión, ambas encriptadas en la llave del server) hacia el server. e) La llave de sesión ahora compartida por el cliente y el servidor, es utilizada para autentificar al cliente y opcionalmente puede ser usada para autentificar al servidor. Esta tecnica es tambien utilizada para encriptar lo referente a communicaciones entre dos nodos.
Llave de encripción	Parametro que en conjunto con el algoritmo de encripcion permiten la protección de información durante su almacenamiento y transmision.
Medida de seguridad	Mecanismos de protección desarrollados en hardware, software, firmware y procedimientos con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información.
Modelo	Es la representacion de un sistema particular en una forma logica, en donde se representan sus componentes e interrelaciones.
Monitoreo	Deteccion, registro y notificación directa de eventos de seguridad ocurridos fuera de los parametros establecidos.
Norma	Modelo; Regla de conducta.
Norma de alcance Organizacional.	Son mandatos expresos acerca de algo que ha de hacerse respecto a situaciones concretas. Se incluyen sólo aquellas que aseguren orienten con mayor precision a la politica de alcance organizacional. EJEMPLO: *"El Comité de Dirección es el único que puede autorizar la plantilla de personal y sus posibles modificaciones"*
Norma especifica:	Son reglas de manera clara y precisa y señalan la decision y la accion a seguir ante una situacion determinada. Difunden alcances y límites de actuación. EJEMPLO: *"Proceso de Selección. Todos aquellos candidatos que ingresen deben cumplir satisfactoriamente los requisitos establecidos en el proceso de selección de personal"*.
PBX (Private Branch eXchange)	Es un sistema telefónico interno que interconecta extensiones una con otra haciendo una especie de red telefónica (conmutador). Puede incluir funciones como costear las llamadas externas, retrollamadas, conferencias y cargos por llamadas internas. Los PBX modernos utilizan todos los métodos digitales para cambiar y manejar terminales digitales y enlazar teléfonos digitales con analógicos.
Pieza de seguridad	Esquema conceptual que define las funciones y elementos de seguridad de un rubro de seguridad en particular.
Pistas de auditoria	Conjunto de registros que de manera agrupada proveen de evidencias documentales en materia de seguridad.
Politica	Arte de conducir un asunto para alcanzar un fin.
Políticas de alcance Organizacional	Son criterios de caracter general formulados para guiar el pensamiento estratégico en la toma de decisiones. Tradicionalmente se presentan de manera resumida, precisa y directa. EJEMPLO: *"Es política de la empresa considerar a su personal como uno de los recursos más valiosos con los que cuenta para el cumplimiento de los objetivos de la misma"*.
Políticas específicas	Son directrices plenamente definidas que orientan cada una de las actividades hacia el logro de los objetivos particulares de las entidades de la empresa en el desempeño de sus funciones. EJEMPLO: *"Es política del departamento de reclutamiento de personal de la empresa, identificar y atraer únicamente al personal cuya ideología, valores y características personales específicas se ajusten a los perfiles de puestos, principios, cultura, objetivos y planes de la empresa"*.

Propietario	Es el director, gerente o representante de la administracion (comúnmente el originador de la información) el cual es responsable de realizar y communicar juicios y decisiones en nombre de la organización con el derecho de uso, identificación, clasificación y protección de un bien informático específico.
Pública (Información)	Información distribuida y ofrecida dentro y fuera de la Institución a los clientes de la Institución.
Recursos Informáticos	Componentes de hardware, software y medios de almacenamiento que permiten el procesamiento y almacenamiento de aplicaciones y datos.
Redundancia	Capacidad que permite duplicar cuantas veces sea necesario aplicaciones, datos y recursos informáticos.
Reporte de excepciones	Información sobre eventos significativos de seguridad registrados en las bitácoras de los sistemas para su análisis y seguimiento.
Respaldo	Provisiones realizadas para la recuperacion de datos, aplicaciones y servicios después de ocurrir una falla o un desastre
Riesgo	Probabilidad de que ocurra algún evento, cuyos efectos vayan en contra de la entidad o sus intereses.
Ruteo	Camino que sigue una transaccion o mensaje a través de la red de comunicaciones.
Socket	Es un API para comunicar una aplicacion y TCP/IP.
Software nocivo	Código indebido que afecta o daña los recursos informáticos, programas y datos.
Shoulder surfers	Fisgón, mirón. Persona observadora con fines de dolo. Shoulder Surfing es la practica de disimuladamente observar a un usuario de un teléfono público cuando digita su número de tarjeta para realizar una llamada telefónica; tomando estos datos los aprovecha o los vende con la finalidad de utilizarlos para realizar llamadas de larga distancia "fraudulentas".
Token	Mecanismo generador de tickes o señales (en nuestro caso claves de acceso y Passwords). Es un código de acceso alfanumérico, usualmente generado con algoritmos indescifrables como el DES, que puede reflejarse en una pieza de software o de hardware. U password es algo que se conoce, un token es algo que se tienen como por ejemplo una llave.
Transacción	Operación manejada por las aplicaciones para la transferencia, actualización y consulta de información.
Usuario	Es una persona que está autorizada por el propietario para hacer uso de los recursos en el cumplimiento de sus funciones.
Validación	Verificación de la validez de la información de acuerdo a los requerimientos establecidos.
Vulnerabilidad	Debilidad de los procedimientos o controles de seguridad, la cual puede ocasionar que un riesgo se materialize.

BIBLIOGRAFÍA

•*DATA SECURITY MANAGEMENT*
AUERBACH PUBLISHERS 1992

•*THE BASELINE APPROACH*
BASELINE GUIDE
SRI INTERNATIONAL 1993

•*INFORMATION SYSTEM SECURITY, A PRACTITIONER'S REFERENCE*
PHILIP FITES, MARTIN P.J. KRATZ
VAN NOSTRAND REINHOLD, 1993

•*COMPUTER SECURITY BASICS*
DEBORAH RUSSELL AND G.T. GANGEMI SR.
O'REILLY & ASSOCIATES, INC., 1991

•*INFORMATION SECURITY HANDBOOK*
WILLIAM CAELLI, DENNIS LONGLEY, MICHAEL SHAIN
STOCKTON PRESS, 1991

•*COMPUTER SECURITY WITHIN ORGANIZATIONS*
ADRIAN R. WARMAN
MACMILLAN INFORMATION SYSTEMS SERIES

•*INFORMATION SYSTEMS STRATEGIC PLANNING*
COMPUTER TECHNOLOGY RESEARCH CORP.

•*CONTROL OBJECTIVES*
MENKUS, RUTHBERG
EDITOR THE EDP AUDITORS FOUNDATION INC., E.U.A. 1990

•*COMPUTER SECURITY*
CARROL, JOHN M.
EDITORIAL BUTTERWORTH PUBLISHERS, E.U.A. 1987

•*NORMATIVIDAD DE SEGURIDAD Y ADMINISTRACIÓN DE RIESGOS.*
RESPONSABILIDADES EN EL MANEJO DE INFORMACIOIN AUTOMATIZADA
BANCO NACIONAL DE MEXICO, 1995

•*DIFERENTES APUNTES DE CONFERENCIAS EN LA ASOCIACIÓN LATINOAMERICANA DE PROFESIONALES DE SEGURIDAD INFORMATICA, ALAPSI*

•*REVISTA: THE ISSA PASSWORD, "THE ONLY PASSWORD YOU SHOULD SHARE"*

•*GUIA DE CERTIFICACION INTERNACIONAL EN SEGURIDAD INFORMATICA*
ALAPSI, 1996

•*GUIA: CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL*
SHARON K. CUNNINGHAM
CISSP EXAMINATIONI STUDY GUIDE