UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

ANÁLISIS DE RIESGO EN LA GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL INSTITUTO MEXICANO DEL PETRÓLEO.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

D A N I E L G A R C I A G A C H U Z

Director de Tesis: M. C. Uriel Tirado Ríos
Codirector de Tesis: Lic. Esteban Lobato Herrera.

FES ARAGON

Septiembre de 2007

Agradecimientos

“Si por un instante Dios se olvidara de que soy una marioneta de trapo y me regalara un trozo de vida, posiblemente no diría todo lo que pienso, pero en definitiva pensaría todo lo que digo”. (Gabriel García Márquez).

A Dios.
A Jesús el Hijo de Dios por ser mi sentido de vida, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente. Por permitirme llegar a este momento tan especial en mi vida. Por los triunfos y los momentos difíciles y las incontables alegrías que me han enseñado a valorarte cada día más. ¡Gracias!

Agradecer hoy y siempre a mi familia.
A mis padres y hermanos por darme la estabilidad emocional, económica, sentimental; para poder llegar hasta este logro, que definitivamente no hubiese podido ser realidad sin ustedes. Gracias por darme la posibilidad de saber lo que es una FAMILIA, por ser los mejores y estar conmigo incondicionalmente, gracias porque sin sus enseñanzas no estaría aquí ni sería quien soy ahora, a ustedes les dedico esta tesis. ¡Gracias!

A mi Papa.
Por los ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, a quien le debo todo en la vida, le agradezco el cariño, la comprensión, la paciencia y el apoyo que me brindó para culminar mi carrera profesional. ¡Gracias!

A ti Mama.
Por haberme educado y soportar mis errores, por soportar todas las preocupaciones y apuraciones que te cause por mi inquietud, y por el corazón que me diste. ¡Gracias!

A Daniela Belem.
A mi porción de cielo que bajó hasta acá para hacerme el hombre más feliz y realizado del mundo, gracias porque nunca pensé que de tan pequeño cuerpecito emanara tanta fuerza y entusiasmo para sacar adelante a alguien. ¡Gracias!

A Rosa Isela.
A la mujer, que dispuso su cuerpo para entregarme este angelito a los nueve meses, también este triunfo es tuyo, te amo. ¡Gracias!

A mis Hermanos
Por que siempre he contado con ellos para todo, gracias a la confianza que siempre nos hemos tenido; por el apoyo y amistad. ¡Gracias!

Al Dr. Uriel Tirado Ríos *por asesorarme a lo largo de la tesis, darme la oportunidad de realizar este trabajo y acompañarme en este camino que hoy culmina en el presente proyecto, por compartir su conocimiento conmigo e inspirar en mi mucha admiración. ¡Gracias!*

A mi director de tesis Lic. Esteban Lobato Herrera *por su asesoría y dirección en el trabajo de investigación. ¡Gracias!*

Al M. en C. Leobardo Hernández Audelo *por su enseñanza en todo el tiempo que estuve en el laboratorio de Seguridad Informática del Centro Tecnológico Aragón é impulsar en mi el gusto por la seguridad informática, y en base a eso me decidí a realizar este trabajo de tesis. ¡Gracias!*

A mis profesores *que me ayudaron en la revisión y corrección de esta tesis. ¡Gracias!*

A todos los profesores *que me dieron clase a lo largo de mi carrera. ¡Gracias!*

A todos mis amigos *por ayudarme a crecer y madurar como persona y por estar siempre conmigo apoyándome en todos las circunstancias posibles. ¡Gracias!*

Al Instituto Mexicano del Petróleo *por permitirme realizar este trabajo de tesis en sus instalaciones y con sus instalaciones. ¡Gracias!*

A la Universidad Nacional Autónoma de México *y en especial a la Faculta de Estudios Superiores Aragón por permitirme ser parte de una gran institución, lo cual me enorgullece el haber pertenecido a esta gran escuela y ser parte de una generación que esta haciendo cosas importantes para el país. ¡Gracias!*

Daniel García Gachuz.

ÍNDICE

Introducción.

La información es un recurso importante para cualquier empresa, ha llegado a tomar un valor importante dentro de las empresas por lo cual debe ser protegida *con base en su valor*. El objetivo principal de la seguridad de la información es proteger la información de una amplia gama de amenazas, a fin de garantizar la continuidad del negocio, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

La información existe en muchas formas: impresa, escrita en papel, almacenada de manera electrónica (cd, disco duro, diskette, etc.), transmitida electrónicamente(correo, ftp, telnet, etc.), presentada en imágenes, o expuesta de manera verbal en una conversación. En cualquier forma que se encuentre la información debe ser protegida adecuadamente tomando en cuenta su valor monetario e importancia para la empresa.

La seguridad en cualquier sistema debe ser proporcional con sus riesgos. Sin embargo, el proceso para determinarse qué controles de seguridad son apropiados y rentables, es a menudo una cuestión compleja y subjetiva. El análisis operacional del riesgo es un componente esencial que debe estar sobre una base objetiva, y así permitir que el riesgo sea manejado con eficacia.

El proceso generalmente consta primero en identifica los impactos potenciales del negocio debido a la indisponibilidad, la pérdida de integridad, y la divulgación de la confidencialidad, así como el valor de los activos del negocio. Los impactos identificados se utilizan para determinar qué áreas y asuntos deben ser considerados a futuro. Este acoplamiento es extremadamente importante, pues se utiliza para justificar recomendaciones y conclusiones.

Las políticas de seguridad de información son la piedra angular de la eficacia de la seguridad de la información.

Sin una política sobre la cual basar los estándares y procedimientos, las desiciones probablemente puedan ser contrarias y estarían presentes las vulnerabilidades de la seguridad listas para ser explotadas por personas internas y externas de igual manera, podría decirse que más internas que externas.

Las políticas de seguridad de información proporcionan una gama extensa de las políticas que se pueden adoptar y modificar por la organización y sobre cuáles puede ser construida una cultura comprensiva de la seguridad de la información.

Estas políticas de seguridad de información son un paso importante hacia un ambiente consciente de la seguridad comprensiva, constante y significativa dentro de la organización.
Un punto a destacar en la aplicación de las políticas de seguridad es que todos los usuarios de la información dentro de su organización entenderán sus responsabilidades y deberes.

Introducción.

La seguridad de la información se puede alcanzar con la preservación de las siguientes características:

a) **Confidencialidad:** Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
   Este servicio de seguridad consiste en garantizar que la información sólo pueda ser accedida por las partes autorizadas para ello y por nadie más. En algunos contextos este servicio se conoce también como privacia.

b) **Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
   Esta sirve a los activos del sistema para prevenir modificaciones, alteraciones, borrado, inserción y, en general, contra todo tipo de acción que atente contra la integridad de los activos.

c) **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.
   Los objetivos de la disponibilidad de datos y de recursos son: respuesta puntual, asignación justa, tolerancia a fallas, utilidad o usabilidad y concurrencia controlada.

d) **Control de Acceso:** Se garantiza la protección de los activos del sistema contra accesos y usos no autorizados.
   Este es de los servicios que normalmente no utilizan técnicas criptográficas para su implementación; en cambio, existe un gran número de técnicas propias y tipos de control de acceso, así como también modelos específicos para su implementación. Este servicio está cercanamente relacionado al de autenticación ya que un usuario debe ser autenticado antes de tener acceso a los activos del sistema.

e) **Autenticación:** Se garantiza que la información provenga de fuentes autorizadas. Este servicio consiste en garantizar que las partes o entidades participantes en una comunicación sean las que dicen ser. Es decir, consiste básicamente en el proceso de identificación de una parte ante las demás, de una manera in controversial y demostrable.

En general, la seguridad de un sistema tiene que ver con cualquier técnica, procedimiento o medida que reduce la vulnerabilidad del sistema. La seguridad tiene como objetivos principales lograr la confidencialidad, integridad, autenticidad de la información y garantizar la disponibilidad de la misma y de los recursos de cómputo.

¿Cómo se puede lograr esto? normalmente para poder asegurar que su información está segura debe realizar un análisis de los posibles riesgos a los que se enfrenta su empresa a diario y solucionarlos. Anteriormente los análisis de riesgos se realizaban de una manera muy compleja y sin ningún documento especifico que sirviera como base para darle mas objetividad, y así poder asegurar que los recursos empleados en la eliminación de riesgos eran los adecuados.

El análisis de riesgos es parte de un esquema de seguridad, el cual tiene la finalidad de poder llegar a implementar un sistema (ISMS) sistema administrativo de seguridad de la información, podría calificarse al análisis de

riesgos como la parte medular para poder realizar la implementación de dicho sistema, sin dejar de mencionar que esto es un producto que consta de diferentes partes: el análisis de riesgos, la administración de riesgos y las políticas de seguridad.

Actualmente los responsables de la seguridad en las empresas ya cuentan con un documento hecho específicamente para la administración de la seguridad dicho documento consta de dos partes:

La primera parte ya es un estándar internacional y se llama ISO17799-1 el cual es un código de prácticas para la administración de la seguridad de la información, es una colección de controles los cuales incluyen las mejores prácticas en seguridad de la información.

La segunda parte está siendo revisada por la organización ISO (Organización Internacional de Normas Técnicas) y se llama BS7799-2, BS por ser un estándar británico, proporciona las recomendaciones para la Administración de Seguridad de la Información a los responsables de iniciar, implementar y mantener la seguridad en la organización. Este es el documento con el cual se evalúa a una compañía que pretende ser certificada.

Este trabajo de tesis tomó como objetivo principal realizar el análisis de riesgos basado en el ISO17799-1 y el BS7799-2, sin dejar de realizar el análisis de riesgos convencional.

1. ISO17799

1.1 INTRODUCCIÓN

Los administradores de seguridad de la información han esperado mucho tiempo a que alguien produjera un conjunto de normas de seguridad de la información mundialmente que estuviera sujeto a auditoria y fuera reconocido globalmente. Se cree que un código de normas de la seguridad apoyaría los esfuerzos de los gerentes de tecnología de la información en el sentido de que facilitaría la toma de decisión de compra, incrementaría la cooperación entre los múltiples departamentos por ser la seguridad el interés común y ayudaría a consolidar la seguridad como prioridad empresarial.[1].

En 1995 el BSI(Instituto Británico de Normas Técnicas) publicó la primer norma de seguridad, BS 7799, la cual fue redactada con la finalidad de que abarcara los asuntos de seguridad relacionados con el comercio electrónico.

Cuatro años después en mayo de 1999, el BSI intentó publicar su segunda versión de la norma BS 7799, la cual fue una revisión más amplia de la primera publicación, sufrió muchas mejoras, en este momento la ISO (Organización Internacional de Normas Técnicas) se percatan de estos cambios y comenzó a trabajar en la revisión de la norma técnica.

En diciembre de 2000, La Organización Internacional de Normas Técnicas (ISO) adoptó y publicó la primer parte de su norma BS 7799 bajo el nombre de ISO 17799, esta norma no incluye la segunda parte de BS 7799, que se refiere a la implementación y la cual no trataremos en este trabajo de tesis.

La norma ISO 17799 es una compilación de recomendaciones para las prácticas exitosas de la seguridad que todas las organizaciones pueden aplicar independientemente de su tamaño o sector, así mismo fue redactada para ser flexible y las recomendaciones son neutrales en cuanto a la tecnología y no ayuda a evaluar y a entender las medidas de seguridad existentes.

1.1.1 ¿Qué es el ISO 17799?

Es una colección de controles que incluye las mejores prácticas en seguridad de la información.
Su intención es servir como punto de partida y referencia para identificar todos los controles necesarios en la mayoría de las situaciones en que los sistemas de información se ven involucrados en la industria y el comercio, esto no implica que se tengan que adoptar todos los controles existentes dentro de la norma pues varia dependiendo de la infraestructura de cada empresa y de los servicios que se otorguen por la misma.

1.1.2 ¿En qué consiste el ISO 17799?

El ISO 17799 está formado por 10 secciones principales de las cuales cada una cubre áreas o tópicos diferentes. [2] Las cuales se mencionan a continuación:

1.1.2.1 (1).- Políticas de Seguridad

Esta sección tiene como objetivo:

Proporcionar dirección y apoyo gerencial para brindar la seguridad de la información.
El nivel gerencial debe establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una política de seguridad de la información através de toda la organización.

1.1.2.2 (2).- Seguridad de la Organización

Esta sección tiene como objetivo:

Administrar la seguridad de la información dentro de la organización.
Mantener la seguridad de las instalaciones de procesamiento de la información y los activos informáticos accesados por terceros, (proveedores, clientes, etc.).
Mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información es ejecutada por terceros(outsourcing).

Debe establecerse un marco gerencial para iniciar y controlar la implementación de la seguridad dentro de la organización. Deben establecerse adecuados foros de gestión liderados por niveles gerenciales, a fin de aprobar la política de seguridad de la información, asignar funciones de seguridad y coordinar la implementación de la seguridad en toda la organización. Si resulta necesario, se debe establecer y hacer accesible dentro de la organización, una fuente de asesoramiento especializado en materia de seguridad de la información.

Deben desarrollarse contactos con especialistas externos en materia de seguridad para estar al corriente de las tendencias de la industria, monitorear estándares y métodos de evaluación y proveer puntos de enlace adecuados al afrontar incidentes de seguridad. Se debe alentar la aplicación de un enfoque multidisciplinario de la seguridad de la información, por ej., comprometiendo la cooperación y colaboración de gerentes, usuarios, administradores, diseñadores de aplicaciones, auditores y personal de seguridad, y expertos en áreas como seguros y administración de riesgos.

1.1.2.4 (3).- Clasificación y Control de Activos

Esta sección tiene como objetivo:

Mantener la protección adecuada de los activos corporativos y garantizar que los activos informáticos reciban un nivel adecuado de protección.

Se debe rendir cuentas por todos los recursos de información importantes y de debe designar un propietario para cada uno de ellos. La rendición de cuentas por los activos ayuda a garantizar que se mantenga una adecuada protección. Se deben identificar a los propietarios para todos los activos importantes y se

debe asignarse la responsabilidad por el mantenimiento de los controles apropiados. La responsabilidad por la implementación de los controles puede ser delegada.

En último término, el propietario designado del activo debe rendir cuentas por el mismo.

1.1.2.5 (4).- Seguridad del Personal

Esta sección tiene como objetivo:

Reducir los riesgos de error humano, robo, fraude, abuso de la información, sistemas y equipos.
Asegurarse que el personal esté consiente de las amenazas a la información y sus implicaciones.
Apoyar la política corporativa de seguridad en contra de accidentes y fallas.

Las responsabilidades en materia de seguridad deben ser explicativas en la etapa de reclutamiento, incluidas en los contratos y monitoreadas durante el desempeño del individuo como empleado.

Los candidatos a ocupar los puestos de trabajo deben ser adecuadamente seleccionados, especialmente si se trata de tareas críticas. Todos los empleados y usuarios externos de las instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad (no divulgación).

1.1.2.6 (5).- Seguridad Física y Ambiental

Esta sección tiene como objetivo:

Impedir accesos no autorizados, daños e interferencias en las instalaciones e información de la empresa.

Las instalaciones de procesamiento de información crítica o sensible de la empresa deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con vallas de seguridad y controles de acceso apropiados. Deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones.

La protección provista debe ser proporcional a los riesgos identificados. Se recomienda la implementación de políticas de escritorios y pantallas limpias para reducir el riesgo de acceso no autorizado o de daño a papeles, medios de almacenamiento, etc.

1.1.2.7 (6).- Administración de las Operaciones y Equipo de cómputo

Esta sección tiene como objetivo:

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
Minimizar el riesgo de fallas en el sistema.

Proteger la integridad del software y la información.
Mantener la integridad y disponibilidad del procesamiento de la información y comunicaciones.
Asegurar la protección de la información en la red y de la infraestructura que la soporta.
Prevenir el daño a los activos y procesos críticos del negocio.
Prevenir la pérdida, modificación o mal uso de la información intercambiada.

Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información. Esto incluye el desarrollo de instrucciones operativas y procedimientos apropiados de respuesta a incidentes.

Se debe implementar la separación de funciones, cuando corresponda, a fin de reducir el riesgo del uso negligente o mal uso deliberado del sistema.

1.1.2.8 (7).- Sistemas de Control de Acceso

Los objetivos de esta sección son:

Controlar el acceso a la información.
Prevenir los accesos no autorizados a sistemas de información.
Garantizar la protección de servicios.
Prevenir los accesos no autorizados a las computadoras.
Detectar actividades no autorizadas.
Garantizar la seguridad de la información.

El acceso a la información y los procesos del negocio deben ser controlados sobre la base de los requerimientos de la seguridad y del negocio.
Para esta se deben tener en cuenta las políticas de difusión y autorización de la información.

1.1.2.9 (8).- Desarrollo y mantenimiento de sistemas

Esta sección tiene como objetivo:

Asegurar que la seguridad es incorporada a los sistemas.
Esto incluirá infraestructura, aplicaciones comerciales y aplicaciones desarrolladas por el usuario. El diseño e implementación de los procesos comerciales que apoyen la aplicación o servicio pueden ser cruciales para la seguridad.

Los requerimientos de seguridad deben ser identificados y probados antes del desarrollo de los sistemas de información. Todos los requerimientos de seguridad, incluyendo la necesidad de planes de reanudación, deben ser identificados en la fase de requerimientos de un proyecto y justificados, aprobados y documentados como una parte de la totalidad del caso del negocio de un sistema de información.

1.1.2.10 (9).- Planeación de la continuidad del negocio

Esta sección tiene como objetivo:

Contrarrestar las interrupciones de las actividades productivas y proteger los procesos críticos del negocio de los efectos de fallas significativas o desastres.

Se debe implementar un proceso de administración de la continuidad de los negocios para reducir la discontinuidad ocasionada por desastres y fallas de seguridad (que pueden ser el resultado de desastres naturales, accidentes, fallas en el equipamiento, y acciones deliberadas) a un nivel aceptable mediante una combinación de controles preventivos y de recuperación.

Así como analizar las consecuencias de desastres, fallas de seguridad e interrupciones del servicio. Se deben desarrollar e implementar planes de contingencia para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.

La administración de la continuidad de los negocios debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

1.1.2.11 (10).- Cumplimiento

Esta sección tiene como objetivo:

Evitar infringir cualquier norma civil o penal, ley, reglamento, obligación contractual o requerimiento de seguridad.
Asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad.
Maximizar la efectividad y minimizar las interferencias hacia y del sistema de auditoria del proceso.

El diseño, operación, uso y administración de los sistemas de información pueden estar sujetos a requisitos de seguridad legal, normativa y contractual.

Se debe procurar asesoramiento sobre requisitos legales específicos por parte de los asesores jurídicos de la organización, o de abogados convenientemente calificados.

Los requisitos legales varían según el país y en relación con la información que se genera en un país y se transmite a otro (por ej. Flujo de datos a través de fronteras).

1.2 ANÁLISIS DE RIESGOS

La Seguridad Informática tiene como objetivo el mantenimiento de la confidencialidad, integridad, disponibilidad, autenticación y control de acceso de los Sistemas de Información.

Es necesario identificar y controlar cualquier evento que pueda afectar negativamente a cualquiera de estos aspectos, así como definir e implantar las defensas necesarias para eliminar o reducir sus posibles consecuencias.
Para ello, deben utilizarse métodos formales de análisis de riesgos que lo garanticen.

1.2.1 Sus Componentes

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

1.2.1.1 Sistema de Información

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

El primer paso en un análisis del riesgo es identificar todas las cosas (activos) que necesitan ser protegidas. Algunas cosas son obvias, como la información propia valiosa, y todas las piezas de hardware; pero, algunos se pasan por alto, por ejemplo la gente que utiliza realmente los sistemas. Lo esencial es enumerar todas las cosas que se podrían afectar por un problema de la seguridad.

Una lista de posibles activos a proteger es sugerida dentro del RFC2196 [3]entre los que se incluyen:

Hardware: CPUs, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, discos duros, líneas de comunicaciones, tableros, terminales de servidores, ruteadores.

Software: Programas fuente, programas objeto, aplicaciones, programas de diagnóstico, sistemas operativos, programas de comunicación.

Datos: Durante la ejecución, almacenada en línea, archivada fuera de línea, respaldos, registros de auditoria, bases de datos, en medios de comunicación de tránsito excesivo.

Gente: Usuarios, administradores, personal de mantenimiento de hardware.

Documentación: De programas, hardware, sistema, procedimientos administrativos locales.

Fuentes: papel, formas, cintas, medios magnéticos.

1.2.1.2 Activos

Definición

Los Activos son los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

La Seguridad de los Sistemas de Información no puede dejar de tenerse en cuenta pues dichos sistemas afectan en la operación correcta de los sistemas organizacionales mantenidos y que son afectados por las decisiones de la Organización.

Cada Activo o bien un conjunto homogéneo de Activos, o bien el Dominio en estudio o el área donde se realizará el análisis de riesgos se caracteriza por su estado en materia de seguridad; estado que se concreta estimando los niveles de Autenticación, Confidencialidad, Integridad y Disponibilidad (A-C-I-D).

1.2.1.3 Vulnerabilidad

Definición

Vulnerabilidad de un activo es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
Cualquier debilidad en los Sistemas de Información e infraestructura que pueda permitir a las amenazas causarles daño y producir pérdidas a la empresa.

La vulnerabilidad es una propiedad de la relación entre un activo y una amenaza. La vulnerabilidad se ha venido vinculando más al activo como una falta de calidad de éste, pero se puede utilizar con una mayor vinculación a la Amenaza cuando el problema lo considere conveniente.

1.2.1.4 Impacto

Definición

Es la medición y valoración del daño que podría producir a la empresa la materialización de una amenaza sobre los Sistemas de Información. La valoración global se obtendrá sumando el costo de reposición de los daños tangibles y la estimación, que siempre será subjetiva, de los daños intangibles.
El Impacto en un Activo es la consecuencia sobre éste de la materialización de una Amenaza.
El Impacto es, visto de una manera dinámica, la diferencia en las estimaciones del estado de seguridad del Activo obtenidas antes y después de la agresión o materialización de la Amenaza sobre éste. Dicho de otra forma, la Amenaza produce en el estado de seguridad del Activo afectado un cambio a un nuevo estado posterior, midiendo el impacto la diferencia entre ambos estados.

1.2.1.5 Riesgo

Definición

Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema de Información, causando un impacto en la empresa.
El riesgo es la posibilidad de que se produzca un impacto determinado en un Activo, en una área o en toda la Organización.

El Riesgo es el resultado del Análisis de Riesgos, un proceso complejo que parte de la determinación de los elementos autónomos, los Activos del área en cuestión y las Amenazas actuantes en él y prosigue con la estimación de los elementos derivados de las Vulnerabilidades y los Impactos mencionados anteriormente.

1.2.1.6 Defensa, Salvaguarda o Contramedida

Definición

Se define la Defensa, Salvaguardas o Contramedidas como la acción que reduce el Riesgo que puede ser un procedimiento o dispositivo, físico o lógico.
Cualquier medio, físico o lógico, empleado para eliminar o reducir un riesgo o eliminar una vulnerabilidad.

Para reducir el riesgo, se necesita la mejora de las salvaguardas existentes o la incorporación de otras nuevas.

1.2.2 La Realización del Análisis de Riesgos

En el proceso de Análisis de riesgos se pueden diferenciar:

Un primer análisis de riesgos será mucho más costoso que los sucesivos.
Puede requerir mucho tiempo y la participación de personal calificado y especializado. El tiempo empleado estará en proporción a los objetivos fijados y a su ámbito de cobertura.

Para resaltar la necesidad de sucesivos análisis de riesgos se deben tener en cuenta las siguientes consideraciones:

Los elementos que componen los Sistemas de Información de una empresa están sometidos a constantes variaciones: nuevo personal informático, nuevas instalaciones, nuevos productos, nuevas aplicaciones, etc.

Pueden aparecer nuevas amenazas o variar la probabilidad de que ocurra alguna de las existentes, afectando al posible impacto.

Pueden aparecer nuevas vulnerabilidades o variar, también pueden llegar a desaparecer alguna de las existentes, creando o eliminando posibles amenazas.

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

Se recomienda implementar el ciclo de mejora continua, el cual parte cuando termina el Análisis de Riesgos previo, se sugiere que entre el último Análisis de Riesgos realizado y el siguiente tenga como máximo un año de distancia, lo ideal es que se realice enseguida el ciclo de mejora continua.

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

1.2.2.1 Definición de Análisis de Riesgos [4]

En un entorno informático existe un conjunto de recursos o activos, humanos, técnicos, de infraestructura que están expuestos a diferentes tipos de Riesgos:

Los normales aquellos comunes a cualquier entorno, y los excepcionales, originados por situaciones concretas que afectan o pueden afectar a parte de una organización o a toda la misma. Para tratar de minimizar los efectos de un problema de seguridad se realiza lo que denominamos un **Análisis de Riesgos**, término que hace referencia al proceso necesario para responder a las siguientes cuestiones básicas sobre nuestra seguridad:

Las siguientes preguntas definen el Análisis de Riesgos.

¿Que queremos proteger? **Activos**

¿Contra quien o qué lo queremos proteger? **Amenaza**

¿Cómo lo queremos proteger?

¿Que puede suceder? **Riesgo.**

Sí sucede ¿qué tanto daño causaría? **Impacto.**

¿Que se puede hacer? **Defensa.**

¿Cuánto va a costar?

¿Vale la pena hacerlo? **Costo – Beneficio.**

El proceso de análisis de riesgos tiene varias fases las cuales se mencionan a continuación:

Identificación y clasificación de los **activos.**

Valoración de los activos.

Identificación y clasificación de los riesgos.

Identificación y clasificación de **vulnerabilidades**.

Correlación de vulnerabilidad y riesgo.

Identificación de los mecanismos de reducción de vulnerabilidades.

Valoración de los mecanismos.

Análisis del beneficio logrado con el costo estimado.

1.2.2.2 Evaluación de los Riesgos en Materia de Seguridad[5]

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. Los valores de recuperación derivadas de la satisfacción de las necesidades de control deben ser equilibradas con respecto al impacto potencial de las fallas de seguridad en los negocios en otras palabras no deben implementarse controles que cuesten mas del valor del activo. Las técnicas de evaluación de riesgos pueden aplicarse a toda la organización, o sólo a partes de la misma, así como a los sistemas de información individuales, componentes de sistemas o servicios específicos cuando esto resulte factible, viable y provechoso.

La Evaluación de Riesgos, orientada a determinar los Sistemas de Información que, en su conjunto o en cualquiera de sus partes, puedan verse afectados directa o indirectamente por amenazas, valorándose todos los riesgos y estableciendo sus distintos niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la empresa.

La Evaluación de Riesgos es una consideración sistemática de los siguientes puntos;

a) **Impacto** potencial de una falla de seguridad en los negocios, teniendo en cuenta las potenciales consecuencias por una pérdida de la autenticidad, confidencialidad, integridad o disponibilidad de la información y otros recursos.
b) **Probabilidad** de ocurrencia de dicha falla tomando en cuenta las amenazas y vulnerabilidades predominantes, y los controles actualmente implementados.

1.3 LAS GUIAS ISO/IEC

Describen así los siguientes pasos del modelo de procesos para la realización del Análisis de Riesgos: [6]

1.3.1.1 Identificación y Requerimientos de protección de Activos

El valor financiero en el libro contable, o de reposición, no es normalmente el que más importa a la Organización, sino que le sigue una pérdida de autenticidad, disponibilidad, integridad o confidencialidad. Este valor define el nivel de protección y los recursos que la Organización quiere dedicarle o emplear en él.

Autenticación. Se define como la característica de dar y reconocer la autenticidad de los Activos de tipo Información y/o la identidad de los actores y/o la autorización por parte de los que autorizan, así como la verificación de las tres cuestiones mencionadas no se ha mencionado el control de accesos ya que esta ligado a la autenticación.

Confidencialidad. Se define como la característica que previene contra la divulgación no autorizada de activos. Concierne sobre todo a Activos de tipo Información, y a menudo se relaciona con la intimidad o privacidad, cuando esa información se refiere a personas físicas. El término divulgación debe tomarse en su sentido más estricto: el simple acceso físico o lógico al activo altera este estado, aunque no haya modificaciones aparentes ni difusión posterior (ataque pasivo).

Integridad. Se define como la característica que previene contra la modificación o destrucción no autorizada. La integridad está vinculada a la fiabilidad funcional del sistema de información o sea su eficacia para cumplir las funciones del sistema de la organización mantenido por él, y suele referirse a Activos de tipo Información. Por ejemplo, son típicos los problemas causados por la amenaza de un virus, llegado en un disquete externo o por la red correo a la integridad de los datos almacenados en el disco duro de una PC.

Disponibilidad. Se define como la característica que previene contra la denegación no autorizada de acceso. La disponibilidad se asocia a la fiabilidad técnica de los componentes del sistema de información, garantiza el funcionamiento al 100% de los servicios dados por la empresa.

Cada Activo o Grupo de Activos incorpora como atributos esenciales dos indicadores sobre dos tipos de valoraciones, que ofrecen una orientación para calcular el posible impacto que la materialización de una amenaza puede provocar en el activo:

1.3.1.2 La valoración intrínseca al Activo

Considerado que tiene dos aspectos:

Uno cualitativo como **valor de uso** del Activo; este atributo permite responder al para qué sirve el Activo y soporta la clasificación anterior en tipos por naturaleza.

Otro cuantitativo como **valor de cambio,** o sea cuánto vale; este atributo es válido para ciertos tipos de Activo y útil tanto a efectos indirectos de la

valoración del Impacto causado por las amenazas, como para soportar la decisión entre la valoración del Riesgo y la de las salvaguardas para reducirlo.

1.3.1.3 La valoración del estado de seguridad del Activo

Considerado como característica por su importancia, se concreta en sus 4 estados **A-C-I-D**: autenticación, confidencialidad, integridad, disponibilidad mencionados anteriormente.

1.3.1.4 Tipos

Se manejaran 5 tipos de o categorías de activos

1.- El entorno del sistema de información, abarca los activos que se necesitan para garantizar los siguientes niveles.

Activos relacionados con el nivel del **Entorno o infraestructura:**
- Equipamientos y suministros (energía, climatización, comunicaciones)
- Personal (de dirección, de operación, de desarrollo, otro)
- Otros tangibles (edificaciones, mobiliario, instalación física)

2.- El sistema de información como tal.

Activos relacionados con el nivel de los **Sistemas de Información:**
- Hardware (de proceso, de almacenamiento, de interfaz, servidores, otros)
- Software (de base, paquetes, producción de aplicaciones, etc.)
- Comunicaciones (redes propias, servicios, componentes de conexión, etc.)

3.- La información tratada por las aplicaciones del sistema de información.

Activos relacionados con el nivel de la **Información:**
- Datos (informatizados, concurrentes al o resultantes del Sistema de Información)
- Meta información (estructuración, formatos, códigos, claves de cifrado)
- Soportes (tratables informáticamente, no tratables)

4.- Las funciones de la organización, que justifican los sistemas de información antes mencionados y les dan finalidad.

Activos relacionados con el nivel de las **Funciones de la organización:**
- Objetivos y misión de la organización.
- Bienes y servicios producidos.
- Personal usuario y/o destinatario de los bienes o servicios producidos.

5.- Otros activos, ya que el tratamiento de los activos en un método de evaluación de riesgos debe permitir la inclusión de cualquier activo, sea cual sea su naturaleza (esta amplia concepción de Activo está en línea con las Guías Prenormativas ISO/IEC, para las que Activo es todo lo que posee o usa una organización).

Otros Activos no relacionados con los niveles anteriores.

- Credibilidad (ética, jurídico, etc.) o buena imagen de una persona jurídica o física.
- Conocimiento acumulado.
- Independencia de criterio o de actuación.
- Intimidad de una persona física.
- Integridad material de las personas, etc.

1.3.1.5 Las métricas de valoración intrínseca de los Activos

Se apoyan en estas situaciones:

Ciertos Activos pueden estar **inventariados**: una parte importante de los Activos de los niveles 1 (**Entorno**) y 2 (**Sistema de información**) pueden tomarse de los Inventarios mantenidos en la empresa y por tanto seguirán las clasificaciones de dichos inventarios (relacionadas a menudo con su contabilidad patrimonial).

Otros Activos pueden estar inventariados o no: así las Aplicaciones existentes que cubren la obtención de determinada Información (nivel 3) o ciertas Funciones de la Organización (nivel 4) suelen estar inventariadas si se compran en el mercado o si se pueden valorar, por ejemplo por su costo de producción.

Una parte de los Activos del Sistema en estudio no son inventariables en el sentido de forma contable, es decir como valor de cambio (por ejemplo para reposición en caso de deterioro). No por ello dejan de tener un valor de uso para la Organización, que a menudo se suele apreciar cualitativamente por su carencia.

No es recomendada la mezcla de valoraciones de activos inventariables y no inventariables porque esta mezcla suele subestimar éstos últimos, sobre todo los inmateriales y especialmente los ligados a la Administración Pública.

Debe intentarse encontrar el valor de cambio del activo como valor de reposición, directa valor de inventario o indirectamente costo de su regeneración tras un Impacto.

Si esa valoración no se pudiera realizar (valor de reposición) de una persona tras un accidente causado por falta de seguridad de algún activo, debe de tratarse este activo con sus posibles impactos y riesgo consecuentes como un elemento del entorno abarcado por el proyecto de seguridad.

1.3.1.6 Las métricas de valoración del estado de seguridad del Activo

Permiten estimar los niveles de sus 4 **estados A-C-I-D** (autenticación, confidencialidad, integridad, disponibilidad).

Estado A de Autenticación. Su escala está ligada a la menor o mayor necesidad de formalización, de autorización y de responsabilidad probatoria en el conocimiento o la comunicación de Activos**.** Se establece una escala con 4 niveles (para cada uno se adjunta un ejemplo de tipo de 'correo' tradicional, cuya terminología se mantiene a menudo en el correo electrónico):

Baja: Si no se requiere conocer autor ni responsable de la información Ejemplo; en un impreso por correo no importa mucho la autorización del emisor-origen o el receptor-destino ni la responsabilidad sobre el contenido.

Normal: Si se requiere conocer el autor para evitar el repudio de origen en un sobre certificado se importan los datos del emisor y el origen, por ejemplo para dar fe de la fecha para un congreso de seguridad.

Alta: Si se requiere además evitar el repudio en el destino (en un sobre con acuse de recibo se importan los datos del receptor y el destino, por ejemplo para dar fe de la fecha para una notificación y no se pueda decir que no se le notificó).

Crítica: Si se requiere además la certificación del autor y del contenido por Ejemplo; una notificación administrativa, para asegurar que el receptor recibe un contenido determinado.

Estado C de Confidencialidad de la Información. Se usa una escala con 4 niveles;

Libre: sin restricciones en su difusión (datos de carácter NO personal)

Restringida: con restricciones normales (dato de carácter personal)

Protegida: con restricciones altas, dato especialmente protegido o sensible, por ejemplo sobre ideología, religión, salud, etc.

Confidencial: no difundible por su carácter crítico.

Estado I de Integridad. Su escala usa 4 niveles, referidos a una característica práctica, la mayor o menor facilidad de volver a obtener el Activo con calidad suficiente**,** o sea completo y no alterado para el uso que se le desea da.

Bajo: si se puede reemplazar fácilmente con un Activo de igual calidad, por ejemplo, información redundante o imprecisa.

Normal: si se puede reemplazar con un Activo de calidad semejante con una molestia razonable.
Alto: si la calidad necesaria es difícil de recuperar y costosa.

Crítico, si no se puede volver a obtenerse una calidad semejante.

Estado D de Disponibilidad. Su escala emplea niveles definidos por el período de tiempo máximo de carencia del Activo sin que las consecuencias o Impactos sean graves para la Organización. Se usa una escala de 4 niveles para los sistemas de gestión habituales en los sectores público y privado:

Menos de una hora: considerado como fácilmente recuperable.

Hasta un día laborable: coincidente con un plazo habitual de recuperación con ayuda telefónica de especialistas externos o de reposición con existencia local.

Hasta una semana: coincidente con un plazo normal de recuperación grave con ayuda presencial de especialistas externos, de reposición sin existencia local o con el arranque desde el centro alternativo.

Más de una semana: considerado como interrupción catastrófica

Otros sistemas tienen tiempos máximos de carencia distintos, que por ejemplo son inferiores a una centésima de segundo para un ordenador embarcado en un satélite; o a una décima para el controlador de una unidad de vigilancia intensiva hospitalaria; o a un segundo en una sala de contratación bursátil electrónica; o a diez segundos en cualquier transacción; etc. En ciertos sistemas, la carencia es menos aceptable en unos períodos que en otros, nóminas a fin de mes, balances en torno al fin de año, etc.

Las escalas y niveles de estos estados de seguridad son adaptables por un especialista en seguridad al dominio concreto estudiado, si fuese conveniente dado lo que se ha mencionado anteriormente que no todos los controles son aplicables a todas las organizaciones.

Se pueden crear grupos de Activos, distintos según cada caso estudiado el nivel de profundidad que sea adecuado a lo previsto en la especificación del Análisis de Riesgos.

Esta descomposición puede permitir la identificación y definición directas de los Activos y/o componentes específicos del objeto estudiado, lo que facilita la colaboración entre las partes involucradas en seguridad y los usuarios.

1.3.1.7 Grupos de Activos según su Amenaza

Susceptibles de ataque por una Amenaza común; así como Grupos de Activos según Salvaguarda, que permitan aplicarles una Salvaguarda común.

La **matriz de activos** comprende columnas para su identificación, uso principal, dependencias y Valores distintos referentes a su autenticidad, disponibilidad, integridad, confidencialidad o ausencia posible de cada una de ellas y recomienda retirar los Activos que muestran valores bajos de Requerimiento de Protección.

1.3.2 EL ANÁLISIS DE AMENAZAS

Enlaza todas las Amenazas a cada Activo; es imprescindible que no se olvide ninguna amenaza importante, lo que causaría fallos en la selección de salvaguardas o debilidades del en el Análisis de Riesgos.

Una amenaza necesita explotar una vulnerabilidad existente para poder atacar un sistema. La comprensión de la naturaleza de los distintos tipos de amenaza (activa, pasiva, accidental, deliberada, etc.) proporciona el grado de protección requerido o necesario, para cada categoría de amenaza hay que identificar: su fuente, tipo y otros factores individuales como por qué existe la amenaza.

Las amenazas están evolucionando y su grado de conocimiento va aumentando, en ciertos casos pueden ayudar las estadísticas, por ejemplo en número de tormentas por año, de caídas de línea por año, de fallas por sistema, etc.

1.3.2.1 Tipos

Los cuatro tipos de amenazas a ese flujo son:

1. **Intersección (**Amenaza al estado de ***confidencialidad):*** una parte no autorizada, un agresor, directamente o por medio de un programa o una computadora obtiene acceso a un factor estratégico.
Ejemplos: intervenir líneas para capturar datos, captura electromagnética, copiado ilícito de programas o archivos de datos.

2. **Modificación (**Amenaza a la ***integridad):*** una parte no autorizada, agresor no sólo obtiene acceso sino que puede manipular este activo. Ejemplos: cambiar valores en un archivo de datos, alteración de un programa para que opere de forma diferente, modificación del contenido de los mensajes que se transmiten en una red, etc.

3. **Fabricación (**Amenaza básicamente a la ***Autenticación):*** Una parte no autorizada, agresor o atacante inserta objetos falsos en el sistema. Ejemplos: inserción de mensajes espúreos en la red, adición de registros a un archivo o base de datos etc.

4. **Interrupción (**Amenaza a la ***disponibilidad):*** un factor estratégico del sistema se destruye o deja de ser accesible o de estar disponible. Ejemplos: destrucción de un componente de hardware como por ejemplo un disco duro, corte de una línea o enlace de comunicaciones, inhabilitación del sistema de gestión de archivos, borrado de un programa o de un archivo de datos etc.

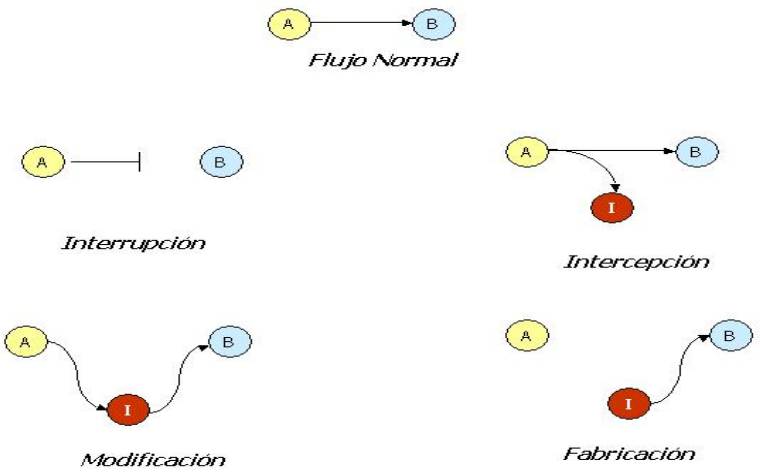

Figura 1.
Amenazas. [7].

Las amenazas intencionales de la red se clasifican en **pasivas y activas** aporta una orientación adicional sobre su funcionamiento y el de las salvaguardas para reducirlas.

1.3.2.2 Amenazas pasivas

La principal amenaza pasiva es de tipo **Intercepción** es la escucha clandestina o la monitorización de la transmisión de información que da al agresor la información que se transmite.
Esta revelación es muy difícil de detectar ya que no altera los datos; el objetivo de los controles contra esta amenaza pasiva es, más que la detección, la prevención del ataque, por reducción de la vulnerabilidad del activo agredido. Se identifican dos formas de esa amenaza pasiva:

Conocimiento o entrega del Contenido del Mensaje, si el agresor lee el contenido de una transmisión por ejemplo un mensaje de Correo Electrónico.

Análisis del Tráfico, si el agresor observa el patrón de la secuencia de los mensajes, y así definir información a partir de la observación del flujo de tráfico para deducir la naturaleza y contenido de la comunicación y puede determinar la localización e identidad de las computadoras que se comunican, así como la frecuencia, tipo de protocolos utilizados y longitud de los mensajes intercambiados (por medio de un Sniffers).

1.3.2.3 Amenazas activas

Las amenazas activas suponen modificación del flujo de datos o creación de un flujo falso, con características opuestas a las de las pasivas. Es difícil prevenir ataques activos dado que primero fueron activos y no se detectaron, para impedirlos, ya que se requeriría protección física de todas las instalaciones y caminos de comunicación en todo momento.

El objetivo en los ataques activos consiste en detectarlos y recuperarse del impacto, ya sea pérdida, interrupción o retardo que puedan causar.

Los otros tres tipos de amenazas citados ***(modificación, fabricación, interrupción)*** se identifican como activas y se extiende la amenaza a la autenticidad.

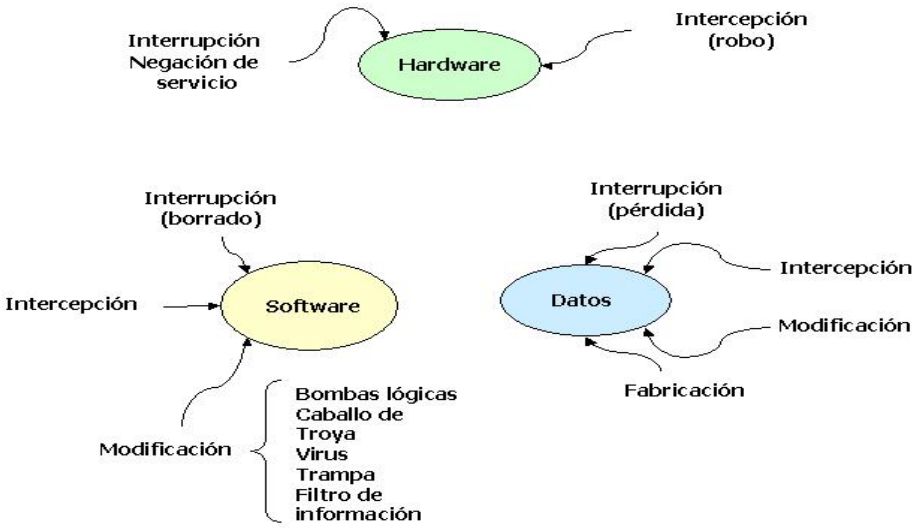

Figura 2.
Amenazas al software, hardware y datos. [7].

A continuación se mencionan algunas de las posibles amenaza a modo de ejemplo:

Modificación de mensajes (contra la Integridad), cuando el contenido de una transmisión de datos se altera sin detección y produce un efecto no autorizado, el agresor captura un mensaje legítimo y altera alguna parte o bien retarda o reordena los mensajes para producir un efecto no autorizado.

Enmascaramiento o suplantación (contra la Autenticidad), una entidad finge ser otra diferente. Un ataque de Enmascaramiento suele incluir otras formas de ataque activo. Por ejemplo, se capturan y repiten secuencias de autenticación después de que se haya realizado una secuencia de autentificación válida, para conseguir que una entidad autorizada con pocos privilegios obtenga privilegios adicionales suplantando a una entidad que los posea.

Repetición (contra la Autenticidad), el agresor repite un mensaje o parte de él por ejemplo, con información de autenticación para producir un acto no autorizado, autenticarse como alguien que no es. Implica la captura pasiva de unidades de datos y su retransmisión.

Denegación de Servicio y DDoS. (Contra la Disponibilidad), el agresor impide o inhibe, retarda operaciones de tiempo crítico, la utilización normal o la

gestión de las instalaciones de comunicaciones; sea un objetivo específico, por ejemplo, suprimir todos los mensajes dirigidos a una dirección o destino dado como el Servicio de Auditoría de Seguridad, sea trastornando una red entera, inhabilitándola o bien sobrecargándola con mensajes para degradar su rendimiento.

La diversidad de causas de las Amenazas permite clasificarlas según su naturaleza, lo que a su vez podrá orientarnos sobre las medidas a tomar para neutralizarlas con cierta autonomía sobre sus consecuencias.

Esta es otro tipo de clasificación en las que se considera cuatro tipos de Amenazas, estas siempre están relacionadas con las anteriores: **No humanas** (accidentes); **Humanas pero involuntarias** (errores); **Humanas intencionales** que necesitan presencia física; y **Humanas intencionales** que no necesitan presencia física de Origen Remoto.

1.3.2.4 No humanas (accidentes)

Accidente físico de origen industrial: incendio, explosión, inundación por roturas, contaminación por industrias cercanas o emisiones radio eléctricas.
Falla: de origen físico o lógico, debida a un defecto de origen o durante el funcionamiento del sistema.
Accidente físico de origen natural: fenómeno sísmico o volcánico, meteoro, movimiento de tierras, avalancha, derrumbe.
Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicación, etc.
Accidentes mecánicos o electromagnéticos: choque, caída, cuerpo extraño, radiación, electrostática.

1.3.2.5 Humanas pero involuntarias (errores)

Errores de utilización: ocurridos durante la recolección y transmisión de datos por el sistema.
Errores de diseño: existentes desde los procesos de desarrollo del software.
Errores de ruta, secuencia o entrega de la información en tránsito.
Inadecuada monitorización, registro del tráfico de información.

1.3.2.6 Amenazas Intencionales Presénciales

Acceso físico no autorizado con inutilización por destrucción o sustracción de equipos, accesorios o infraestructura.
Acceso lógico no autorizado con intercepción pasiva simple de la información, requiere sólo su lectura.
Acceso lógico no autorizado con alteración o sustracción de la información en tránsito o de configuración, requiere lectura y escritura, es decir, reducción de la confidencialidad del sistema para obtener bienes o servicios aprovechables, programas, datos, etc.
Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración.

Indisponibilidad de recursos, sean humanos, huelga, abandono, rotación o técnicos, desvío del uso del sistema, bloqueo.

1.3.2.7 Amenazas Intencionales de Origen Remoto

Acceso lógico no autorizado con intercepción pasiva, para análisis de tráfico.
Acceso lógico no autorizado con modificación o destrucción de información en tránsito o de configuración, requiere lectura y escritura, y usando o no un reemisor, es decir, reducción de la integridad y/o disponibilidad del sistema sin provecho directo, sabotaje inmaterial, infección por virus.
Acceso lógico no autorizado con modificación, Inserción, Repetición de información en tránsito.
Suplantación de Origen del emisor o reemisor, o de Identidad.
Repudio del Origen o de la Recepción de información en tránsito.

El elemento Amenaza no tiene atributos destacables que sean útiles para el Análisis y Gestión de Riesgos, siempre debe de tomarse en cuenta que no todas las amenazas operan dentro de su empresa, deben seleccionarse únicamente las que tengan relación directa con su empresa.

La ocurrencia intrínseca de la amenaza tiene sólo un interés genérico si no está asociada como agresión materializada.

Al Activo agredido pese a todo, puede ayudar a valorar la Vulnerabilidad que concreta dicha asociación por excepción, o sea si no hubiera valoración específica de dicha Vulnerabilidad, en este caso se expresa según la siguiente escala:

Periodo medio de ocurrencias, Valor en la escala.

- menor de una vez por semana Frecuencia muy alta
- menor que a cada 2 meses Frecuencia alta
- menor que un año Frecuencia media
- menor que 6 años Frecuencia baja
- mayor que 6 años Frecuencia muy baja

La escala escogida no se basa en consideraciones objetivas, sino que intenta contrarrestar los efectos de la incertidumbre en la determinación de los períodos en base a los intervalos que aproximadamente se aumentan de forma exponencial y con relación a los sucesos dentro de la empresa.

La **Matriz de Amenazas** añade a la columna de Activos las posibles amenazas ligadas a cada componente, relativas a la autenticidad, disponibilidad, integridad o confidencialidad, así como una columna con los daños posibles al Activo.

Funciones / Amenazas	Amenaza 1	Amenaza 2	...
Función 1	DV11=[A,M,B] DI11=[A,M,B]	DV12=[A,M,B] DI12=[A,M,B]	
Función 2	DV21=[A,M,B] DI21=[A,M,B]	DV22=[A,M,B] DI22=[A,M,B]	
...			

Figura 3.
[6] Criterios y sugerencias.

Esta grafica es un ejemplo de cómo se relacionan las amenazas con las funciones que se desempeñan.

Agrupación de los posibles eventos o amenazas en escenarios. Cada escenario conlleva un conjunto de amenazas que pueden atacar a un conjunto de activos y producir ciertos tipos de impacto.

Grupos Jerárquicos de Amenazas/agresiones, distintos según el caso estudiado y hasta el nivel de detalle que sea para el agrupamiento de Activos y a la fase de estudio. La descomposición debe permitir la identificación y definición de las agresiones al mismo nivel de detalle de los Activos y/o componentes específicos del Objeto estudiado, lo que facilita la colaboración entre los expertos de seguridad y los usuarios.

Grupos de Amenazas/agresiones según los estados de Seguridad citados en los Activos. Ciertas Amenazas atentan exclusiva o predominantemente contra el estado de Autenticación, por ejemplo la suplantación del Origen de un mensaje; otras contra el estado de Confidencialidad, por ejemplo consulta no autorizada, otras contra el de Disponibilidad, indisponibilidad de personal imprescindible o sistemas claves, o el de Integridad, pérdida de datos en una transmisión.

Se mencionan diferentes tipos de técnicas con tal de hacer más fácil y exacto el análisis de amenazas, recordando nuevamente que depende del escenario en que se encuentre que es el que indica las que se deben utilizar.

1.3.3 EL ANÁLISIS DE LAS VULNERABILIDADES

Cada Activo implica considerar cada una de las vulnerabilidades en conjunto con la amenaza posible que pueda explotarla, sin la implantación de la correspondiente salvaguarda.

La Vulnerabilidad es un concepto con dos aspectos:

• La Vulnerabilidad como propiedad ejerce una función de mediación entre la Amenaza como acción y el Activo como objeto de cambio del estado

de seguridad. Por este aspecto estático la Vulnerabilidad forma parte del estado de seguridad del Activo.

• La Vulnerabilidad es asimismo en su aspecto dinámico, el mecanismo obligado del paso o conversión de la Amenaza a una agresión materializada sobre un Activo.

Por poner ejemplos, la Amenaza, Inundación por desbordamiento de torrente combinada con el Activo centro de procesamiento de datos situado en una zona inundable, se plasma en una Vulnerabilidad de dicho Activo respecto a esa Amenaza. Esta Vulnerabilidad depende del propio ciclo de frecuencia de las avenidas en la zona y de la ubicación del propio centro de procesamiento de datos (cercanía, situación en un sótano, etc.).

Es una confusión muy frecuente combatir, la asimilación de la Vulnerabilidad como una probabilidad, empleando el concepto de potencial y potencialidad en general como más cercano al tránsito de una amenaza materializables en agresión. La potencialidad se convierte en frecuencia para los casos de calculo definido y en posibilidad para los casos de calculo difuso.

1.3.3.1 Tipos

Se consideran dos tipos principales.

• La **Vulnerabilidad intrínseca** del Activo respecto al tipo de Amenaza sólo depende de estas dos entidades, Activo y Amenaza en este caso no se toman en cuenta los controles de seguridad que puedan estar implementados por el activo.

• La **Vulnerabilidad efectiva** del Activo tiene en cuenta las Salvaguardas o controles de seguridad aplicadas en cada momento a dicho Activo y se tiene en cuenta en forma de un factor que estima la eficacia global de dichas Salvaguardas.

La Vulnerabilidad no tiene otra clasificación distinta a la que le otorgan sus factores propios; en todo caso se clasifica dé acuerdo con el Activo y la Amenaza a los que está estrechamente asociada.

Sólo para evitar la inmanejable explosión de las posibles combinaciones de todas las posibles amenazas sobre todos los activos mantenidos, conviene organizar ambas entidades en grupos o bien centrarse en las amenazas más fácilmente materializables y/o más impactantes sobre los Activos amenazados dadas las inter-relaciones tanto entre amenazas como entre activos.

1.3.3.2 Vulnerabilidad Intrínseca

La vulnerabilidad intrínseca puede descomponerse, si conviene y para análisis muy detallados (sobre todo de amenaza intencional), según dos bloques de atributos:

• **Potencialidad autónoma** respecto al Activo amenazado de ocurrencia de la Amenaza (por ejemplo la frecuencia de inundaciones en un lugar determinado).

• **Potencialidad derivada** de la relación entre Activo y Amenaza (**intencional** sobre todo)

• **Factores subjetivos** generadores de más o menos '**fuerza'** (motivación, disuasión)

• **Oportunidad de acceso a el área** con capacidad y recursos, según 4 aspectos:

Acceso físico presencial: número de personas o entidades autorizadas por su función a acceder normalmente al entorno del Activo, con una escala de 4 niveles.
- una sola persona o entidad
- pocas personas de una entidad
- bastantes personas de pocas entidades distintas
- bastantes personas de varias entidades distintas

Acceso físico calificado: calificación, formación general y experiencia de los usuarios autorizados a acceder físicamente al entorno del Activo, con esta escala.
- no se requiere calificación
- se requiere poca formación para manejar la documentación técnica
- se requiere cierta experiencia para manejar la documentación técnica
- se requiere alta formación y experiencia para manejar la documentación técnica

Acceso lógico de competencia: Conocimiento técnico específico sobre el Activo atacable, con una escala de 4 niveles.
- no requiere competencia especial
- es fácil de realizar por un usuario
- requiere la competencia de un desarrollador
- necesita un experto muy calificado

Accesibilidad lógica instrumental: Disponibilidad de los instrumentos que corresponde a la tecnología del Activo amenazado, con una escala de 4 niveles.
- no requiere instrumentos o éste es muy accesible
- no requiere instrumentos especiales pero su acceso es restringido (costo)
- requiere instrumentos especiales aunque accesibles de la tecnología considerada.
-requiere instrumentos especiales y de acceso muy difícil.

La Medición de la Vulnerabilidad consiste en considerar la distancia entre la Amenaza potencial y su materialización como agresión real sobre el Activo.

También se mide la Vulnerabilidad cuando es factible por la frecuencia histórica o bien por la posibilidad de la materialización de la Amenaza sobre el Activo. Para ciertos Activos existen datos cuantitativos precisos, como son: la fiabilidad de un componente de hardware, número de fallos del software etc.

Pero como en general estas medidas no están disponibles, una primera aproximación cualitativa a la frecuencia o posibilidad de materialización de la Amenaza lleva a emplear la escala vista en las Amenazas potenciales, consideradas como reales, o agresiones.

Periodo medio	**Escala subjetiva**	**Escalas objetivas**
menos que 1 semana	Frecuencia	muy alta ≅ 0.2 ≅ 50
menos que 2 meses	Frecuencia	alta ≅ 0.02 ≅ 5
menos que 1 año	Frecuencia	media ≅ 0.002 ≅ 1
menos que 6 años	Frecuencia	baja ≅ 0.0002 ≅ 0.2
superior a 6 años	Frecuencia	muy baja ≅ 0 ≅ 0.02

entre ocurrencias por día por año.

Esta medición de Vulnerabilidad no sólo es inviable en muchas ocasiones, sino que puede ser inconveniente para ciertos tipos de sectores, Activos o Amenazas. Sectores como por ejemplo: la defensa, energía nuclear, transporte de personas, etc. ejercen su función como misión y trabajan con Activos que requieren seguridad crítica por su propia naturaleza. En estos casos la Vulnerabilidad para una amenaza es un mecanismo nulo, no le afecta o todo el riesgo es el propio impacto pleno.

La descomposición de la Vulnerabilidad intrínseca en Potencialidad genérica de ocurrencia de la Amenaza y Acceso de la Amenaza al área nos indica una métrica de Vulnerabilidad que combina la medición anterior, para la posibilidad generalizada con una corrección por factores incrementadores que tienen en cuenta las Accesos.

La Vulnerabilidad no tiene otra clasificación distinta a la que le otorgan sus factores propios; en todo caso se clasifica de acuerdo con el Activo y la Amenaza a los que está estrechamente asociada. Sólo para evitar la inmanejable explosión de las posibles combinaciones de todas las posibles amenazas sobre todos los activos involucrados, conviene organizar ambas entidades en Grupos o bien centrarse en las amenazas más fácilmente materializables y/o más impactantes sobre los Activos amenazados.

1.3.3.3 Ejemplos:

Como por ejemplo las siguientes:

Vulnerabilidades Físicas.

Esta relacionado con poder acceder físicamente al sistema para robar, manipular o destruir el mismo.

Vulnerabilidades de Hardware y Software.

Existen ciertos dispositivos físicos que son más vulnerables que otros, como por ejemplo hubs frente a switches, o algunas placas de red. Lo mismo ocurre con la parte de Software. Existen sistemas operativos más seguros que otros y diversos programas con los que sucede lo mismo.

Vulnerabilidades por Emanación.

Si bien no son tan comunes o al menos difundidas, aquel que aplique un sistema de defensa con intensidad Paranoica deberá tenerlo en cuenta. Este punto trata sobre dispositivos electrónicos que emiten radiaciones que pueden ser descifradas o reconstruidas.

Vulnerabilidades por Comunicaciones.

La conexión de ordenadores dentro de un entorno aumenta el grado de vulnerabilidad. El compartir recursos, la conexión a Internet, abren puertas de acceso que debemos tener muy en cuenta.

Vulnerabilidad Humana.

Que puede dividirse en dos ramas.

* *Intencionales.*
* *Accidentales.*

La **Matriz de Vulnerabilidades** enlaza la lista de Activos-Amenazas con las posibles Vulnerabilidades por pérdida de autenticidad, disponibilidad, integridad o confidencialidad.

1.3.4 EL ANÁLISIS DE IMPACTO

Valora el daño probable por una amenaza a un activo, teniendo en cuenta su vulnerabilidad y sus consecuencias para la Organización.

1.3.4.1 Tipos

Se emplea una tipología de Impactos orientada a la naturaleza de las Consecuencias de las combinaciones Activo-Amenaza, estas combinaciones son tan numerosas que no sería útil tomarlas como causas o naturaleza de los Impactos para clasificarlos, como se hizo con las Amenazas.

Por lo tanto, un mal funcionamiento simple de un Activo no constituye normalmente un Impacto si no contiene una consecuencia de deterioro y prejuicio apreciable como podría ser un cambio de estado. Por ejemplo no se considera Impacto la interrupción del tratamiento de una aplicación en un sistema por un micro-corte de energía, o el reenvío automático de un mensaje por un servicio que tenga mecanismos de auto recuperación.

Se considera tres grandes grupos de Impactos, dependiendo de que sus Consecuencias sean reductoras directamente de los estados de seguridad A-C-I-D del Activo agredido; o bien indirectamente, y en este caso, de forma cuantitativa o cualitativa.

Se ha tomado una parte de los tipos de Impacto que tienen consecuencias sobre los estados del Activo considerado.

1.3.4.2 Impactos con consecuencias cualitativas funcionales

El deterioro del estado de ***Autenticación*** no suele ser evolutivo (multiplicación en cadena) pero produce directamente la anulación de documentos y procedimientos e indirectamente inseguridad jurídica.

• El deterioro del estado de ***Confidencialidad*** no suele ser evolutivo y tiene consecuencias de distintos órdenes, unas directas, como son divulgación de información confidencial o revelada anticipadamente, sustracción puntual o masiva y otras indirectas como, desconfianza, incomodidades, chantaje, pérdida de la confianza del cliente y usuarios, etc.

• El deterioro del estado de ***Integridad*** puede ser evolutivo y tiene consecuencias directas como la alteración de información sensible o vital en mayor o menor escala, e indirectas como la posible contaminación de programas, pérdida, tratamiento erróneo, etc.

• El deterioro del estado de ***Disponibilidad*** puede ser evolutivo y causar de inmediato desde la degradación de la productividad del activo como recurso o la interrupción de su funcionamiento de forma más o menos duradera y profunda, de unos datos, de una aplicación, de un servicio o de todo un sistema. Indirectamente esto se traduce en caída de margen por falta de resultados; así como en gastos suplementarios para recuperar o mantener la funcionalidad anterior a la amenaza.

1.3.4.3 Impactos con consecuencias Cuantitativas

Una parte de los deterioros anteriores tienen Impactos con consecuencias cuantitativas de diversos tipos.

Pérdidas de valor económico, ligadas a activos inmobiliarios o inventariables**,** que comprenden todos los costos de reposición de la funcionalidad, incluyendo los gastos de sustituir, reparar o limpiar lo dañado: edificios y obras, instalaciones, computadoras, redes, accesorios, etc.

Pérdidas indirectas, valuables económicamente y ligadas a activos intangibles en general no inventariados: gastos de transacción y restauración o reposición de elementos no materiales del sistema: datos, programas, documentación**,** procedimientos, etc.

Pérdidas indirectas, valuables económicamente y unidas a disfuncionalidades tangibles: se aprecian por el costo del retraso o interrupción de funciones operacionales de la organización; La interrupción o ruptura de los flujos y ciclos productivos, de productos, servicios o expedientes, por ejemplo, incluido el deterioro de la calidad de éstos, y la incapacidad de complementar las obligaciones contractuales o estatutarias.

Pérdidas económicas relativas a la responsabilidad legal, ya sea, civil, penal o administrativa del propietario o responsable del sistema de información por los perjuicios causados a terceros.

1.3.4.4 Impactos con consecuencias Cualitativas

Otros deterioros de los estados de seguridad tienen Impactos con consecuencias cualitativas orgánicas de varios tipos.

Pérdida de fondos patrimoniales intangibles: conocimientos, documentos, datos o programas no recuperables, información confidencial etc.

Responsabilidad penal por Incumplimiento de obligaciones legales (Revelación de secretos y acceso ilícito a sistemas y equipos de informática “Diario oficial de la nación fecha: 17 de mayo de 1999”) [4] por mencionar alguno.

Perturbación o situación embarazosa político-administrativa, credibilidad, prestigio, competencia política, etc.

Daño a las personas por algún tipo de incidente físico o personal.

Desde el punto de vista de las Consecuencias directas sobre el estado de seguridad del Activo, el Impacto conjunta dos atributos o factores, la gravedad intrínseca del resultado y la o Atenuante circunstancial.
Ambos atributos hacen cambiar al menos uno de los niveles de los 4 estados de seguridad del Activo: A, C, I, o D.

1.3.4.5 Atributos de los Impactos

Desde el punto de vista de las Consecuencias indirectas y como se ha visto, un Impacto tiene como atributo importante:

El aspecto cuantitativo de la consecuencia provocada, sea material, por ejemplo una pérdida monetaria para la reposición, o inmaterial, pérdidas como datos, programas, documentación o procedimientos.

El aspecto cualitativo**,** por ejemplo, pérdidas de fondo de comercio, pérdidas o daño de vidas, situación embarazosa político-administrativa, atentados a la intimidad personal.

Las diferencias en los atributos implican variaciones de medición y tratamiento del Impacto, aunque todas son generalmente cualitativas (por carencia de datos estadísticos cuantitativos)**.**

Se indican dos formas básicas de valorar los impactos, apoyadas ambos en casos cualitativos:

Valoración en tiempo de la falta de **disponibilidad** de algún activo importante.

Valoración en **unidades monetarias** de una escala con niveles meramente orientativos, que representa las cantidades a emplear para reparar los daños producidos por una amenaza materializada en la organización.

Rango de valores en pesos del Impacto.

menor que 100.000 Muy bajo
menor que 1.000.000 Bajo
menor que 10.000.000 Medio
menor que 100.000.000 Alto
mayor que 100.000.000 Muy alto

Estos valores son variables dependiendo de la organización que este en revisión.

La cuantificación de los Impactos es no sólo uno de los procesos más difíciles del Análisis de Riesgos, sino que es el más influyente en el cálculo del propio Riesgo.

Como se verá en el Modelo de Eventos, el nivel del Riesgo depende directamente de la Vulnerabilidad y del Impacto, pero se da a éste un peso mayor por todos los especialistas en el proceso de decisión que apoya al cálculo del riesgo. Es un ejemplo clásico de ordenación de preferencias como cualquiera prefiere, como riesgo menor, un impacto bajo con una vulnerabilidad o potencialidad aunque sea muy alta (perder dinero a la lotería por ejemplo) a un impacto alto por baja que sea su potencialidad o vulnerabilidad (arriesgar la vida por ejemplo).

Por tanto, en un primer intento se escogerá como medida del impacto el costo de reposición del activo dañado. Cuando esta medida no es factible o no tiene sentido, se intentará apreciar el costo de reposición de la función o servicio realizado por el Activo dañado, a partir del deterioro de alguno de sus estados de seguridad.

Así por ejemplo:

La pérdida alta del estado de ***disponibilidad*** de un Activo de tipo información, el cual es difícil recuperar, afecta total o parcialmente a una función de la Organización durante un tiempo determinado, por ejemplo, si se pierde la información sobre los pedidos, se pierde un mes de facturación.

La misma pérdida alta del estado de ***confidencialidad*** no hace perder la facturación actual, pero se puede haber dado la lista de pedidos a un competidor que la usará para hacernos perder clientes y su facturación futura, pérdida posiblemente mucho más alta, si no se toman las medidas adecuadas.

La **Matriz de Impactos** combina las columnas de Amenazas y Activos para añadir los Impactos posibles: La lista combina los datos de los Análisis de Amenazas y Vulnerabilidades ordenadas por tipo de amenaza, eliminando las

filas con menor Impacto y comprimiendo así la lista para retener los pares Amenaza-Activo que muestran un Impacto importante y seguir procesándolos.

1.3.5 EL ANÁLISIS DEL RIESGO

El Riesgo es el resultado del Análisis de Riesgos, un proceso complejo que parte de la determinación de los elementos autónomos o los Activos del área y las Amenazas actuantes en él y prosigue con la estimación de los elementos derivados de las Vulnerabilidades y los Impactos.

Se permite realizar ese Análisis complejo con el objetivo de obtener un resultado concreto: un valor calculado de riesgo que nos permita tomar decisiones para proseguir a la siguiente etapa del proceso de Análisis de Riesgos. Esta decisión puede tomarse por comparación explícita del Riesgo calculado con un nivel prefijado de Riesgo.

El Riesgo calculado es simplemente un indicador ligado al par de valores calculados de la Vulnerabilidad y el Impacto, ambos derivados a su vez de la relación entre el Activo y la Amenaza/agresión a las que el Riesgo calculado se refiere.

1.3.5.1 Tipos

Se diferencia en varios tipos de Riesgo:

El **Riesgo calculado intrínseco:** Se define o calcula antes de aplicar salvaguardas o controles de seguridad, elemento del modelo estudiado en el apartado siguiente.

El **Riesgo calculado residual:** Se considera como el que se da tras la aplicación de salvaguardas o controles de seguridad dispuestas en un escenario de simulación o en el mundo real.

El **Umbral de riesgo:** es un valor establecido como base para decidir por comparación si el Riesgo calculado es asumible o aceptable.

Existen dos tipos de atributos, uno de cada Riesgo y otro de relación entre riesgos:

Restricción a cada tipo de impacto factible dada la vulnerabilidad de un activo o grupo de activos a una amenaza o conjunto de amenazas.

Propagación del riesgo para activos dependientes entre sí.

En el caso más sencillo, la Vulnerabilidad se ha podido estimar como una frecuencia, por ejemplo de fallos de un componente y el impacto también se ha podido apreciar como un valor monetario de reposición de ese componente.
Entonces el Riesgo calculado se puede apreciar por el impacto acumulado durante un período de tiempo, por ejemplo un año.

El Riesgo será así el costo de las reposiciones del componente durante el año y se podrá comparar, bien con un umbral determinado, bien con el costo también anual de las salvaguardas y/o controles para reducirlo. Así, si el componente falla cada mes como media y su reposición cuesta 100.000 pesos, el Riesgo anual será simplemente la composición de ambas cantidades, o sea 1.200.000 pesos.

La medición de Riesgos en este caso sencillo, Vulnerabilidad como frecuencia e Impacto monetarizado será:

Rango de costos anuales en pesos, Riesgo.

- menor que 50.000 Muy bajo
- en torno a 500.000 Bajo
- en torno a 5.000.000 Medio
- en torno a 50.000.000 Alto
- mayor que 100.000.000 Muy alto

En los casos más complejos, cuando la Vulnerabilidad no se puede establecer como frecuencia o el Impacto no se puede monetarizar, se recomienda estimar la medida del Riesgos con ayuda de una tabla cualitativa o su matriz equivalente con los siguientes niveles:

Impacto	RIESGO				
Muy alto	Alto	Muy alto	Muy alto	Muy alto	Muy alto
Alto	Medio	Alto	Alto	Alto	Alto
Medio	Bajo	Bajo	Medio	Medio	Medio
Bajo	Bajo	Bajo	Bajo	Medio	Medio
Muy bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Bajo
Vulnerabilidad	Muy baja	Baja	Media	Alta	Muy alta

Figura 5.
[6]Matriz de Riesgos, Impactos y Vulnerabilidades.

Esta figura nos muestra la relación y valoración del impacto, la vulnerabilidad y el riesgo.

Rango de riesgos, Impacto, Vulnerabilidades (frecuencias).

Si el proyecto tiene como objetivo la realización de un Análisis y administración de Riesgos inicial y genérico, la técnica de cálculo del riesgo se orienta a una discriminación, en dos bloques de los riesgos.

En esta aplicación genérica también se tienen pocos elementos para discriminar las Vulnerabilidades y los Impactos en gran número de niveles, por lo que puede ser no sólo suficiente, sino además lógico, reducir la matriz anterior por ejemplo a los 3 niveles Bajo, Medio y Alto (como indican los recuadros anteriores).

Las diferencias de tipificación entre riesgos calculados intrínsecos o residuales, umbrales de riesgo y riesgos aceptables son irrelevantes a efectos de sus mediciones.

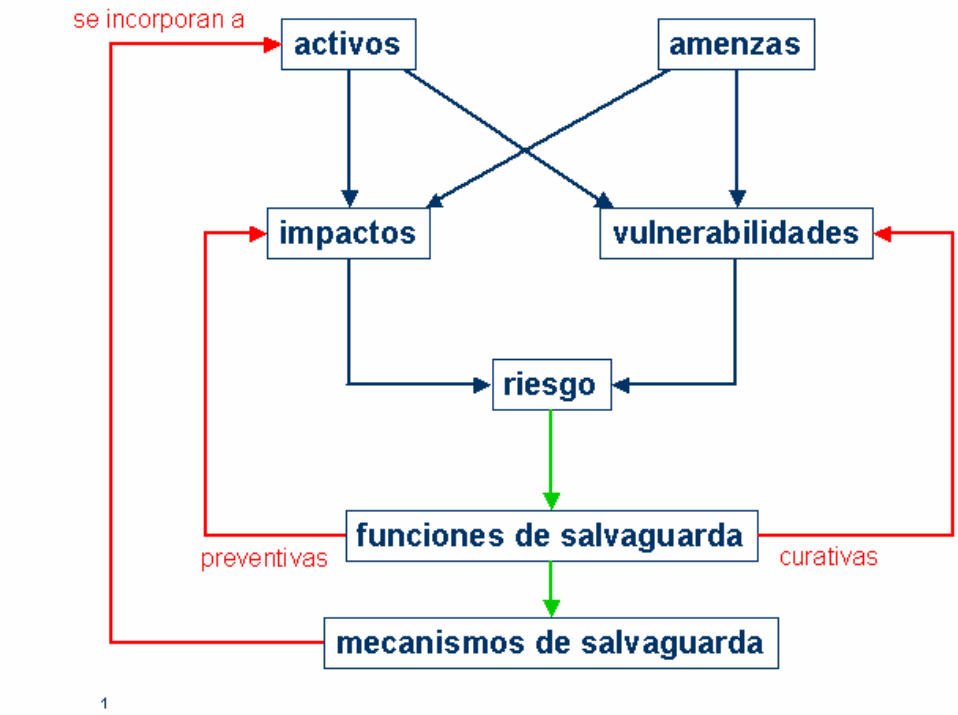

Figura 6.
[8] Elementos del análisis de riesgos.

Esta figura nos muestra como se encuentran relacionados todos os componentes del análisis de riesgos, y como se afectan entre si.

La información correspondiente a las salvaguardas, mecanismos y/o controles de seguridad se incorporan dentro del siguiente tema de tesis, el cual se encarga de la administración de los riesgos y la selección de estos mecanismos.

2. ADMINISTRACIÓN DE RIESGOS

2.1 Introducción

La administración global de Seguridad de un Sistema de Información determinado es una acción permanente, cíclica y recurrente, es decir, se ha de realizar continuamente debido a los cambios del sistema y de su entorno, el cual se descompone en fases sucesivas, las cuales se muestran a continuación.

1. ***Planificación del Proyecto de Riesgos.*** Esta primera fase consiste en las consideraciones iniciales para arrancar el proyecto de análisis y administración de riesgos, se estudia la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el ámbito que abarcará, planificando los medios materiales y humanos para su realización e inicialización del propio lanzamiento del proyecto.

2. ***Análisis de riesgos.*** En esta fase se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral del riesgo deseable.

3. ***Administración de riesgos.*** Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.

Acotación y Estado de seguridad del Área estudiada.

En toda Administración de Seguridad de Sistemas de Información, hay que empezar siempre por acotar el área seleccionada, delimitando los Activos que comprende y separándolos respecto a su entorno, pero sin dejar de considerar su influencia sobre el área. El área se caracteriza por su estado de seguridad que se concreta estimando los niveles de los cuatro estados de seguridad siguientes: Autenticación, Confidencialidad, Integridad y Disponibilidad.

Es prudente no automedicarse sin control médico. Por lo que es aconsejable la consulta racional a especialistas de seguridad, puesto que muchas salvaguardas no se pueden aplicar a todo tipo de dominios o amenazas y han de usarse selectivamente de acuerdo a las circunstancias locales. Por ejemplo alguien que no sea especialista puede pensar que el adquirir una salvaguarda basta para proteger un activo importante, mientras que el especialista puede aconsejar su refuerzo u otra salvaguarda alternativa porque prevé que habrá que contrarrestar niveles de amenazas excepcional o circunstancialmente elevados.[14]

2.1.2 Análisis y Administración de Riesgos[14]

El Análisis y Administración de Riesgos es el ‘corazón’ de toda actuación organizada en materia de seguridad. Influye incluso en las fases y actividades de tipo estratégico de la dirección en sus objetivos, políticas, y condiciona la profundidad de las fases y actividades de tipo logístico como son la planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento.

Capítulo 2 Administración de Riesgos.

Existen diferentes etapas en la administración de riesgos que detallamos enseguida:

De manera general estas son las etapas que deben de abarcarse en un estudio de seguridad completo, al cumplir con todas estas tareas podría decirse que se ha realizado un estudio de seguridad completo.

La etapa de Determinación de **OBJETIVOS, ESTRATEGIA y POLÍTICA** de Seguridad de los Sistemas de Información se nutre y nutre a su vez la etapa de análisis y administración de riesgos.

La etapa de Establecimiento de la **PLANIFICACIÓN** de la Seguridad de los Sistemas de Información deriva de la etapa de análisis y administración de riesgos como su consecuencia funcional más inmediata.

La etapa de Determinación de la **ORGANIZACIÓN** de la Seguridad de los Sistemas de Información deriva de la etapa de análisis y administración de riesgos como su consecuencia orgánica más inmediata.

La etapa de **IMPLANTACIÓN de SALVAGUARDAS** y otras medidas de Seguridad para los Sistemas de Información deriva de las etapas de Planificación y Organización.

La etapa de **CONCIENCIACIÓN de TODOS** en la Seguridad de los Sistemas de Información deriva de las etapas de Planificación y Organización. Tiene en cuenta el papel fundamental del recurso humano interno en todo proyecto de seguridad y usa técnicas generales de administración de Proyectos y administración de Formación, Comunicación y Recursos Humanos.

La etapa de **REACCIÓN** o respuesta a cada evento, **MANEJO y REGISTRO** de las incidencias y de **RECUPERACIÓN** de estados aceptables de Seguridad tiene un carácter básicamente operacional y utiliza técnicas generales de administración cotidiana de seguridad y de atención a sus incidentes. Es el resultado de estudios de Seguridad concretos.

La etapa de **MONITORIZACIÓN, ADMINISTRACIÓN de CONFIGURACIÓN** y de **CAMBIOS** en la Seguridad de los Sistemas de Información tiene un carácter de mantenimiento, con técnicas generales de monitorización, de administración de configuración y administración de cambios adaptadas al ámbito de la seguridad.

Esta misma terminación marca el comienzo de un nuevo estudio de seguridad para continuar con el ciclo de mejora continua por las múltiples razones mencionadas a lo largo de este documento.

A continuación detallaremos el siguiente punto medular que es la administración de los riesgos identificados previamente.

2.2 TAREAS DE LA ADMINISTRACIÓN DE RIESGOS

Las tareas involucradas en la administración de riesgos son:

2.2.1 Adoptar una política de administración de riesgos

Una política de administración de riesgos debe contemplar: la misión de seguridad, las políticas y procedimientos de seguridad, sus objetivos, alcance, restricciones, responsabilidades etc. Esta política rige la implementación de salvaguardas y su control, debe anunciarse, comunicarse y se debe vigilar su adopción individual.

Esta parte del Análisis de Riesgos tiene por objetivo manejar los niveles de riesgo e incertidumbre para cumplir con los objetivos de la empresa definidos y establecidos por los directores principales de la organización o negocio, así como identificar y seleccionar las funciones de salvaguarda apropiadas a un costo razonable para reducir el riesgo a un nivel aceptable.

Es importante mencionar que la Administración de Riesgos no puede ni debe ser completamente la responsabilidad de una sola persona, sino que es una actividad comunal que implica la participación de toda la gente asociada al proyecto.

Los puntos de partida para esta parte están constituidos por la documentación de la etapa anterior, referida a la descripción de los componentes del riesgo: activos, funciones y mecanismos de salvaguarda existentes, amenazas, vulnerabilidades e impactos, a los niveles de riesgos calculados y a los umbrales de riesgo aceptados por los responsables del proyecto.

El proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información: Implica la identificación, selección, aprobación y manejo de las salvaguardas (contra medidas) para eliminar, o reducir a niveles aceptables los riesgos evaluados, con el objetivo de:

Reducir la posibilidad de que una amenaza ocurra.
Limitar el impacto de una amenaza, si ésta se manifiesta.
Reducir o eliminar una vulnerabilidad existente.
Permitir la recuperación del impacto o su transferencia a terceros (contratación de seguros).

2.3 SALVAGUARDAS

Estudios realizados en los últimos años demuestran que un alto porcentaje de organizaciones ha experimentado algún tipo de pérdida de información o soporte físico, siendo las causas más frecuentes los errores no intencionados y los virus y gusanos. Hoy en día, debiera ser impensable tener Pc’s o servidores sin programas de protección contra virus.

El aumento en el número de delitos informáticos está haciendo replantearse a los profesionales de las tecnologías de la información las medidas de seguridad y mecanismos de control.

Capítulo 2 Administración de Riesgos.

Los delitos informáticos se han convertido en un mayor riesgo debido por una parte a que hay un mayor número de personas que conocen la informática y tienen acceso a recursos informáticos, y por otra al alto nivel de interconexiones entre redes tanto internas como externas. Pero sigue ocurriendo que la mayoría de los incidentes se originan interiormente a la organización, tanto los no intencionados como los maliciosos.

La administración de los riegos de seguridad de la organización provee a los gerentes de TI de un enfoque más sistemático para estimar los activos y las vulnerabilidades que existen, evaluar las amenazas y monitorear o auditar la seguridad básica.

Más que un proceso para determinar y controlar la exposición de la empresa al riesgo, la Administración de Riesgos es un proceso para estimar el impacto del riesgo dentro de la seguridad básica de la empresa.

Através de la administración de riesgos los gerentes de TI pueden identificar que riesgos impactarán más significativamente la infraestructura del negocio de la empresa y que gastos en seguridad tendrán preparado el mayor retorno de la inversión.

Hoy en día, la administración de riesgos de seguridad se combina con las distintas fases de la seguridad: Evaluación, Planeación, Implementación y monitoreo o auditoria. El objetivo de esto es producir evaluaciones dirigidas a la administración y recomendaciones que pueden integrarse en la misión general de la empresa, sus objetivos y los del negocio.

Antes de comenzar todo este proceso los administradores de TI deberán definir las razones por las cuales se desea implementar la Administración de Riesgos.

Para muchas empresas, la Administración de Riesgos es parte del enunciado de su misión; por ejemplo, sí una empresa coloca el servicio al cliente como una prioridad máxima, entonces el objetivo de la Administración de Riesgos, podría ser evitar que las que amenazas pudieran interrumpir el servicio.

Es esencial asegurarse de que los controles y el gasto sean completamente proporcional con los riesgos a los cuales se expone la organización.

Sin embargo, muchos métodos convencionales para realizar análisis del riesgo de seguridad están llegando a ser más y más inaceptables en términos de la utilidad, flexibilidad, y críticamente en términos de lo que producen para el usuario.

2.4 Actividades a realizar en esta parte:

Podemos considerar 4 principales actividades a realizar en la administración de riesgos:

1. **Interpretación del riesgo.**

Interpretación de los resultados generados en las actividades anteriores, orientada a descubrir las principales áreas críticas.

2. **Identificación de funciones de salvaguarda y estimación de su efectividad.**

Identificación y estimación de la efectividad de las funciones o servicios de salvaguarda necesarias para reducir el riesgo a los umbrales aceptados.

3. **Selección de las funciones de salvaguarda.**

Selección de las funciones o servicios de salvaguarda óptimos que cumplan los objetivos de reducción del riesgo.

4. **Análisis costo beneficio.**

Estudio de los riesgos residuales obtenidos por la aplicación de las funciones o servicios de salvaguarda seleccionados, para determinar si se encuentran dentro de los umbrales del riesgo elegidos.

2.4.1 Interpretación del riesgo

El punto de partida para esta Actividad está constituido por la documentación de la etapa anterior que describe los componentes del riesgo (activos, funciones y mecanismos de salvaguarda existentes, amenazas, vulnerabilidades e impactos) y los niveles de riesgos calculados.

2.4.1.1 Interpretar y manejar los riesgos

[15]Descripción y objetivo:

Los resultados del cálculo de los riesgos encontrados deben interpretarse antes de poder utilizarlos, agrupándolos con el objeto de identificar las áreas de mayor riesgo, del área y por lo tanto las que necesitan mayor protección.

- El umbral de riesgo es un valor establecido como base para decidir por comparación con él si el riesgo efectivo calculado es asumible o aceptable.

Los umbrales de riesgo utilizados pueden partir de una estimación inicial, establecido por las personas responsables del proyecto y propuesta por similitud respecto a otros casos.
Estos umbrales de riesgo se pueden refinar por aplicación del Análisis y Administración de los Riesgos en un escenario de simulación del equilibrio entre los costos de los riesgos y los de las salvaguardas o controles en un entorno de ciertas

restricciones por parte de la Organización o de su capacidad presupuestaria a corto plazo, por ejemplo.

• Mientras que el Riesgo efectivo calculado no se considere asumible, se propone desarrollar las actividades siguientes de 'Identificación, estimación de efectividad y selección de las funciones de salvaguarda'.

• Cuando el Riesgo efectivo calculado ya se considera asumible, quedará como riesgo residual. Esto también procede a la obtención de indicadores estadísticos sobre frecuencias de ocurrencia de amenazas (vulnerabilidad), amenazas con mayor impacto, áreas más afectadas por mayores riesgos, etc.

La tabla 1. Ilustra cómo puede ser realizado este análisis. La determinación de la probabilidad y de la seriedad de los riesgos en un proyecto proporciona una buena indicación de la exposición del riesgo del mismo.

Riesgo.	**Probabilidad.**			**Severidad ó Criticídad.**		
	Bajo.	Medio.	Alto.	Bajo.	Medio.	Alto.
Pérdida de financiamiento		X		X		
Denegación de servicio distribuido.			X			X
Fallas en los UPS de servidores importantes.		X				X

Tabla 1: *Ejemplo de evaluación de riesgos.*

Este análisis ayuda a los implicados en el proyecto, a identificar cuales son los riesgos más significativos, y por lo tanto cuales son los que necesitan una administración cuidadosa. En la práctica, es a menudo difícil evaluar la probabilidad /severidad de los riesgos cuantificables porqué se utiliza una escala cualitativa de los tópicos regularmente. El significado de las letras utilizadas en estas tablas 2 y 2a. Se mostrara en la tabla 3. Los riesgos evaluados en la tabla 1 se pueden calificar fácilmente usando la matriz del riesgo en la siguiente tabla: 2.

Probabilidad.	**Seriedad.**			
	Bajo.	Medio.	Alto.	
Bajo.	E	D	C	
Medio.	D	C	B	
Alto.	C	B	A	

Tabla 2: *Matriz de riesgos para riesgos clasificados.*

En el caso de proyectos más grandes o más complejos, la matriz se debe ampliar para asegurar que sé calificar en A y se asigna automáticamente a cualquier riesgo definido como seriedad extremadamente alta; es decir, cualquier riesgo que sea realizado, y cause fallas en el proyecto. Un ejemplo se muestra en la siguiente tabla 2a en donde se asigna otro nivel de seriedad.

Probabilidad.	**Seriedad.**			
	Baja.	Medio.	Alta.	EXTREMA
Baja.	E	D	C	A
Media.	D	C	B	A
Alta.	C	B	A	A

Tabla 2a: *Matriz de riesgos para riesgos clasificados.*

Las tablas 2 y 2a, nos muestran la relación entre el valor ofrecido a la probabilidad y seriedad, los cuales generan o se asignan un valor establecido por medio de la letras definidas, a las cuales se les asigna un valor o acción, la cual se define en la tabla siguiente.

Grado.	**Acciones de Mitigación de Riesgo.**
A	Las acciones de mitigación, para reducir la probabilidad y la seriedad, debe ser identificado y puesto en ejecución tan pronto comience el proyecto.
B	Acciones de mitigación, para reducir la probabilidad y la seriedad, debe ser identificado y aplicar acciones apropiadas durante la ejecución del proyecto.
C	Acciones de mitigación, para reducir la probabilidad y la seriedad, debe ser identificado y costeado para posible acción si los recursos lo permiten.
D&E	Debe ser observado; No hay acción necesaria a menos que el grado aumente en un cierto plazo.

Tabla 3: *Acciones recomendadas para los grados del riesgo.*

Frecuentemente, las evaluaciones de riesgos se realizan primero en un nivel alto, a fin de priorizar recursos en áreas de alto riesgo, y posteriormente en un nivel más detallado, con el objeto de abordar riesgos específicos.

Una vez identificados los requerimientos de seguridad, deben seleccionarse e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable.

Los controles pueden seleccionarse sobre la base de algún documento, o de estándares, o pueden diseñarse nuevos controles para satisfacer necesidades específicas según corresponda. No obstante, es necesario reconocer que algunos controles no son aplicables a todos los sistemas o ambientes de información, y podrían no resultar viables en todas las organizaciones.

Los controles deben seleccionarse teniendo en cuenta el costo de implementación en relación con los riesgos a reducir y las pérdidas que podrían producirse de tener lugar una violación de la seguridad. También deben tenerse en cuenta los factores no monetarios, como el daño en la reputación, etc.

2.4.1.2 Consecuencias

La tabla siguiente nos muestra unas medidas cuantitativas con respecta a las consecuencias que se podrían llegar a tener, así como su descripción.

Medida cuantitativa.	**Descripción.**
Catastrófico.	Las consecuencias amenazarían la disposición de los servicios principales, causando problemas importantes para los clientes, el gobierno y la agencia. Pérdida posible mayor de $10 millones.
Mayor.	Las consecuencias amenazarían la disposición eficaz continua de servicios y requerirían la administración del nivel superior o la intervención ministerial. Pérdida posible de entre $5 millones y $10 millones.
Moderado.	Las consecuencias no amenazarían la disposición de servicios, sino significarían que la agencia estaría conforme a revisión o a maneras cambiantes del funcionamiento. Pérdida posible de entre $1 millón y $5 millones.
De menor importancia.	Las consecuencias amenazarían la eficiencia o la eficacia de algunos servicios, pero se podían tratar de internamente. Pérdida posible de entre $100.000 y $1 millón.
Insignificante.	Las consecuencias son ocupadas por funcionamientos generales. Pérdida posible de menos de $100.000.

Tabla 4: *medida cuantitativa por consecuencias.*

Los valores y las oraciones mostradas en la mayoría de las tablas sirven únicamente como ejemplos, en ninguna de ellas se describen como estándares, ya que deben variar dependiendo del giro y tamaño de la organización.[16]

2.4.1.3 Probabilidad

La tabla siguiente nos muestra unas medidas cualitativas con respecta a la probabilidad que se podrían llegar a tener, así como su descripción.

Medida cualitativa.	**Descripción.**
Casi Seguro.	Se espera que el acontecimiento ocurra en la mayoría de las circunstancias(una o más veces por año).
Probablemente	El acontecimiento ocurrirá probablemente en la mayoría de circunstancias(uno o dos años).
Moderado.	El acontecimiento debe ocurrir en una cierta vez (una vez en cinco años).
Poco probable.	El acontecimiento podría ocurrir en un cierto tiempo (una vez en diez años).
Raro.	El acontecimiento puede ocurrir solamente en circunstancias excepcionales (una vez en cincuenta años).

Tabla 5: *medida cualitativa por probabilidad.*

2.4.1.4 Nivel de Riesgo

Esta tabla nos muestra la relación entre las consecuencias y la probabilidad para generar el nivel del riesgo asociado o generado.

	Consecuencias.				
Probabilidad	**Insignificante**	**De menor importancia**	**Moderado.**	**Mayor.**	**Catastrófico.**
Casi Seguro.	H	H	E	E	E
Probablemente	M	H	H	E	E
Moderado.	L	M	H	E	E
Inverosímil.	L	L	M	H	E
Raro.	L	L	M	H	H

Tabla 6: *Relación entre probabilidad y consecuencia.*

E = Riesgo Extremo: Requiere Acción Inmediata.
H = Alto Riesgo: Requiere Atención de la administración mayor.
M = Riesgo Moderado: La administración de responsabilidad debe ser especificada.
L = Riesgo bajo: Manejado por procedimientos de rutina.

Es recomendable utilizar para esto un informe de interpretación del riesgo, así como estimados estadísticos propios de la organización.

2.4.2 Identificación y estimación de funciones y servicios de Salvaguarda

Esta actividad permite identificar las funciones o servicios de salvaguarda que reducen el riesgo, así como estimar su eficacia para lograr dicha reducción.

2.4.2.1 La Selección de Salvaguardas

Debe tener en cuenta diversos tipos de condiciones para poder implantarlas apropiadamente. La lista inicial de salvaguardas se escoge en relación con la identificada medición de riesgos, tras asegurarse de que están justificadas.

Sería inapropiado recomendar salvaguardas más costosas que el valor de los activos que quieren proteger o que el presupuesto asignado para la seguridad por la Organización, que en este caso debe estar consciente del riesgo.

La función o servicio de salvaguarda es una acción de tipo actuación (o de tipo no-actuación, es decir omisión), puesto que surge de una decisión para reducir un riesgo (no es una acción de tipo evento).

Dicha actuación se materializa en el correspondiente mecanismo de salvaguarda que opera de dos formas posibles, en general alternativas:

- ‘Neutralizando’ o ‘bloqueando’ otra acción, que es el evento de materialización de la Amenaza en forma de agresión, con reducción previa al evento de la Vulnerabilidad mediadora de dicha materialización, dicho de otra forma evitar que una amenaza pueda ser explotada eliminando la vulnerabilidad asociada a dicha amenaza.

- Modificando el estado de seguridad del Activo agredido de nuevo (lo había modificado anteriormente por el Impacto consecuente a la Amenaza materializada), con reducción posterior al evento productor de dicho Impacto, dicho de otra forma una activo al ser agredido cambia se estado de seguridad a un estado más bajo, modificar el estado es regresarlo a su anterior nivel de seguridad.

2.4.2.2 Identificar las funciones y servicios de salvaguarda

Descripción y objetivo:

Se propone, sin tomar en consideración ninguna restricción, una lista de las funciones o servicios de salvaguarda que pueden reducir el riesgo superior al umbral en los dominios identificados en la etapa anterior de Análisis de Riesgos.

Las funciones o servicios propuestos se determinan con ayuda de las agrupaciones de activos/amenazas donde se detecta mayor riesgo.

Activos o grupos de activos (entorno, sistema de información, información, funcionalidad, otros), amenazas (accidentes, errores, intencionales presénciales, etc. por la propia función de las funciones y servicios (orientados a la: detección, prevención, corrección, recuperación, concientización de la información).

La lista debe contener la descripción de las características de la función o activo de salvaguarda, por ejemplo: tipo de amenaza, tipo de activo que protegen, a qué estado de seguridad (A-C-I-D: Autenticación, Confidencialidad, Integridad, Disponibilidad) se orientan, resultado (disminución de vulnerabilidad o bien de impacto), etc.

Para poder realizar este punto adecuadamente es necesario contar con una lista de funciones o servicios propuestos por los responsables y colaboradores del proyecto.

2.4.2.3 Tipos de funciones, servicios y mecanismos de salvaguarda

Las funciones, servicios y mecanismos de salvaguarda se tipifican, según su forma de *actuación,* en dos grandes tipos:

• Las funciones o servicios preventivos actúan sobre la Vulnerabilidad (antes de la agresión) y reduce la potencialidad de materialización de la Amenaza (no la posibilidad genérica de ésta, que es independiente del Activo amenazado). Este tipo de función o servicio actúa en general contra amenazas humanas.

• Las funciones o servicios curativos o restablecedoras actúan sobre el Impacto (tras la agresión) y reduce su gravedad. Este tipo de función o servicio actúa en general con amenazas de todos los tipos.

Las salvaguardas no son uniformes para todos los sistemas. El nivel del riesgo debiera determinar el nivel de control adecuado. Cada riesgo se puede tratar mediante la aplicación de uno o varias salvaguardas de seguridad. Las salvaguardas se pueden clasificar también en las siguientes tres principales categorías:

- **Administrativas.**
- **Físicas.**
- **Técnicas.**

Las salvaguardas **administrativas** incluyen las políticas y procedimientos de seguridad.

Las políticas establecen lo que los usuarios pueden y no pueden hacer al utilizar los recursos informáticos de la organización. También incluyen procedimientos para la renovación de claves de acceso, autorizaciones para acceder a sus recursos, la revisión y validación periódica de la vigencia del tipo de acceso, la asignación de responsabilidades, conocimientos de la seguridad y formación técnica, administración y supervisión de las tecnologías y soluciones aplicadas, la

recuperación tras averías o fallas y la realización y aplicación de planes de contingencia.

Los controles administrativos también incluyen la revisión de seguridad e informes de auditoria, que se utilizan para identificar si los usuarios siguen las políticas y procedimientos. Finalmente, los controles administrativos incluyen la asignación de propiedad de los datos y los recursos.

Cada persona de la organización debe de tener claras sus responsabilidades relativas a la seguridad de cada componente a su cuidado, y estas responsabilidades se deben incluir en los objetivos de cada persona para asegurar que se les valore por la responsabilidad asignada y se les evalúe según el cumplimiento de sus obligaciones.

Las salvaguardas **físicas** limitan el acceso físico directo a los equipos. Las salvaguardas físicas consisten en cerraduras, bloqueos para teclados, vigilantes de seguridad, alarmas y sistemas ambientales para la detección de agua, fuego y humo. Las salvaguardas físicas también incluyen sistemas de respaldo y alimentación de reserva, tales como baterías y fuentes de alimentación ininterrumpida (UPS).

Las salvaguardas **técnicas** son controles que se implantan a través de soportes físicos o lógicos que típicamente son difíciles de vencer y, una vez implantados, pueden funcionar sin la intervención humana. El soporte lógico específico incluye antivirus, firmas digitales, cifrado, programas de control de biblioteca, herramientas de administración de red, contraseñas, tarjetas inteligentes, control de acceso de llamadas, sistemas de rellamada, seguimiento de huellas o trazas de auditoria y sistemas expertos de detección de intrusiones.

Los controles de acceso protegen contra la utilización o manipulación no autorizada de recursos mediante la verificación y la autorización. La *verificación* asegura la identidad del usuario o sistema que solicita acceso. Los controles de autorización aseguran que el acceso a la información y los recursos informáticos se limiten de acuerdo con las directrices de la dirección.

Otro término relacionado a la seguridad es el no-repudio. El no-repudio previene la posibilidad de que una de las partes de un intercambio o transacción niegue en falso después que haya tenido lugar la misma. El control técnico que se emplea para garantizar el no-repudio es la firma digital.

Las operaciones comerciales realizadas a través de redes internas e Internet se han vuelto corrientes. Allí donde antes se empleaba una firma manuscrita para verificar que se había hecho una compra o realizado un determinado contrato, ahora existe una alternativa digital para verificar que una persona cumplirá con sus obligaciones.

La firma digital consiste en una clave privada que sólo conoce o puede duplicar el que tenga la clave, parecido a su firma y rúbrica manuscrita. Las firmas digitales verifican la fuente, autenticidad e integridad de mensajes electrónicos.

Las salvaguardas administrativas, físicas y técnicas se pueden subdividir en preventivas y correctivas. Las preventivas intentan evitar la ocurrencia de acontecimientos indeseados, mientras que las salvaguardas correctivas intentan identificar los incidentes y reducir sus efectos después de que hayan sucedido. Es siempre preferible evitar un incidente de seguridad en lugar que tener que hacerle frente a posteriori.

Las salvaguardas correctivas se han diseñado para identificar el problema con suficiente rapidez para reducir los daños al mínimo y para poder valorar con precisión la magnitud de los daños causados por el incidente. La Figura siguiente presenta los controles administrativos, físicos y técnicos específicos, y los clasifica además en mecanismos preventivos o correctivos.

Controles de Seguridad de Información.
Preventivos / Correctivos. **Controles Físicos.** Archivos y documentación de respaldo. Detectores de movimiento. Detectores de humo y fuego. Guardias de seguridad. Monitorización por televisión de circuito cerrado. Sistemas de tarjetas de identificación. Censores y alarmas. Cerraduras y llaves. Candados cifrados. Alimentación eléctrica de reserva. Controles biométricos de acceso. Selección de emplazamiento. Extintores de incendios. Bloqueo de teclados. **Controles Administrativos.** Conocimientos de seguridad y formación técnica. Revisiones y auditorías de seguridad. Separación de obligaciones. Control de calidad. Procedimientos sancionadores. Investigaciones de antecedentes. Políticas y procedimientos de seguridad. Rotación de responsabilidades. Gestión y supervisión. Recuperación de averías y planes de contingencia. Administración de accesos de usuarios. Administración de propietarios de datos y recursos.

Controles Técnicos
Programas de control de acceso Logs y trazas para auditoría. Programas cortafuegos y antivirus. Sistemas expertos de detección de intrusiones. Administración de contraseñas. Tarjetas inteligentes. Cifrado.

Los tres tipos de salvaguardas deben utilizarse conjuntamente para hacer frente a los riesgos estimados en cada entorno concreto de trabajo. La dirección debe decidir cuánto invertir razonablemente en la seguridad, los procedimientos de administración y control, y en herramientas tecnológicas para limitar el riesgo de forma proporcionada y equilibrada.

Las funciones o servicios de salvaguarda, así tipificados según sus formas de actuación, lógicamente pueden clasificarse según:

• Los tipos de Amenazas generadoras de las Vulnerabilidades para las funciones o servicios preventivos.

• Los tipos de Impactos para las funciones o servicios curativos.

Estas dos clasificaciones complementarias según Vulnerabilidades-Amenazas e Impactos tienen la ventaja de facilitar sustancialmente el funcionamiento del modelo de Procedimientos.

Las funciones y servicios de salvaguarda pueden especificarse aún con más detalle dentro de cada gran tipo de salvaguardas preventivas o curativas:

2.4.2.4 Salvaguardas Preventivas

La **Concientización, información y formación** del personal propio y del relacionado establemente con la Organización son un tipo de salvaguarda ‘estructural’ (ligada a la estructura global de la Organización y no sólo a sus Sistemas de Información). Su importancia está justificada por el papel esencial que juega en la seguridad el factor humano.

La **Disuasión** es un tipo de salvaguarda que empuja a que el potencial agresor humano intencional reconsidere el inicio de la agresión, a partir de las consecuencias que puedan sobrevenirle contra su propio interés. Este tipo de salvaguarda exige normalmente una difusión lo más amplia y a su vez selectiva posibles. Por poner ejemplos, el establecimiento de condenas es una de las salvaguardas de disuasión más conocidas.

La **Prevención** propiamente dicha es un tipo de salvaguarda de protección que no impide el inicio de la materialización de la amenaza, sino su realización completa y por lo tanto la consecución plena del impacto. Como ejemplo de salvaguarda preventiva puede tomarse el control de accesos.

La **Detección preventiva** puede llegar a ser hasta disuasoria (sí su instalación es conocida por el potencial agresor, consciente de que podría ser descubierto).

2.4.2.5 Salvaguarda Curativas o Restablecedoras

La **Corrección** es un tipo de salvaguarda que impide la propagación del Impacto. Por ejemplo, un impacto en la integridad de una información detectado por su descuadre lleva a tomar medidas para paralizar la circulación de dicha información y de verificar sus fuentes.

La **Recuperación** es un tipo de salvaguarda restauradora que repara los daños o reconstruye los elementos dañados para acercarse al estado de seguridad del Activo agredido previo a la agresión. Cuando no basta la recuperación funcional, pueden adoptarse también otras salvaguardas como la transferencia del riesgo a terceros (por ejemplo con los seguros) o la acción ante los tribunales.

La **Detección curativa, 'monitorización' o seguimiento curativo** del impacto**,** en caso de amenaza ya materializada, es previa a toda eficacia en la actuación de las salvaguardas curativas (muchas agresiones son detectadas tarde o temprano). El cuadre de la información sería un buen ejemplo de esta salvaguarda detectora.

Los **mecanismos de salvaguarda,** tipificados según sus formas de actuación también como preventivos o curativos, se especifican con más detalle dentro de cada tipo según el **'recurso' empleado** de la Organización (mecanismos organizacionales, físicos, de software específico de seguridad, de contratación de seguros).

Estos recursos a su vez se pueden relacionar estrechamente con los activos o grupos de activos tipificados en este mismo modelo (entorno, sistema de información, información, funcionalidad, otros activos), dando tipos de mecanismos concernientes a la arquitectura básica, los soportes, las comunicaciones, la explotación, la compra de paquetes y el desarrollo de aplicaciones, etc.

Según las organizaciones se van reestructurando y reducen su complejidad para competir en una economía global, es imperativo el empleo de las tecnologías de la información y las comunicaciones para lograr una ventaja competitiva o una mayor eficacia.

La clasificación de mecanismos según los recursos empleados tiene la ventaja de facilitar sustancialmente el funcionamiento del modelo de Procedimientos.

2.4.2.6 Estimar la efectividad de las funciones y servicios de salvaguarda

Descripción y objetivo:

A partir de la lista de funciones y servicios de salvaguarda especificados para los dominios seleccionados en el proyecto, esta tarea procede a estimar su efectividad en la reducción de los elementos integrantes del riesgo (vulnerabilidad e impacto).

Dicha efectividad, es calculada por un especialista, dependiendo de las condiciones:

Objetivas: la complementariedad o contradicción con otras salvaguardas instaladas.

Subjetivas: las restricciones que no se han tenido en cuenta en las partes anteriores.

Aquí será necesario contar con un informe de las funciones o servicios de salvaguardas propuestos con una estimación de su efectividad.

2.4.3 Selección de Funciones y Servicios de Salvaguarda

Esta actividad permite seleccionar las funciones o servicios de salvaguarda convenientes y justificados de acuerdo a los riesgos que deben cubrir.

Los resultados de esta evaluación ayudarán a orientar y a determinar las prioridades y acciones de gestión adecuadas para la administración de los riesgos concernientes a seguridad de la información, y para la implementación de los controles seleccionados a fin de brindar protección contra dichos riesgos.

Puede resultar necesario que el proceso de evaluación de riesgos y selección de controles deba llevarse acabo en varias ocasiones, a fin de cubrir diferentes partes de la organización o sistemas de información individuales.

Es importante llevar a cabo revisiones periódicas de los riesgos de seguridad y de los controles implementados a fin de:

a) Reflejar los cambios en los requerimientos y prioridades de la empresa.
b) Considerar nuevas amenazas y vulnerabilidades.
c) Corroborar que los controles siguen siendo eficaces y apropiados.

Las revisiones deben llevarse a cabo con diferentes niveles de profundidad según los resultados de evaluaciones anteriores y los niveles variables de riesgo que la gerencia está dispuesta a aceptar.

2.4.3.1 Aplicar los parámetros de selección

Descripción y objetivo:

Partiendo de la lista de funciones y servicios de salvaguarda propuestos, y teniendo en cuenta los umbrales de riesgo máximo asumible o aceptable obtenidos en tareas y decisiones anteriores, la tarea es ordena la lista
según su efectividad para reducir el riesgo.

La tarea es seleccionar en el orden establecido las funciones o servicios que reducen el riesgo hasta los umbrales requeridos por el objetivo de seguridad establecido.

2.4.3.2 Características

La **Eficacia genérica** es una característica de una Función o Servicio de Salvaguarda que hace pasar de la **Vulnerabilidad intrínseca** del Activo y el **Impacto pleno** sobre éste a una **Vulnerabilidad** y un **Impacto efectivos** (que son los que tienen en cuenta dicha Función o Servicio).

La **Eficacia concreta** es un atributo de un Mecanismo de Salvaguarda. Esta Eficacia suele ser no específica (reduce el riesgo de distintos Activos) por lo que suele estar asociada a la eficacia de otros Mecanismos de Salvaguarda. También transforma la **Vulnerabilidad intrínseca y el Impacto pleno** del Activo respecto al tipo de Amenaza respectivamente en **Vulnerabilidad e Impacto efectivos** (que son los que tienen en cuenta dicho Mecanismo de Salvaguarda).

2.4.3.3 Métricas

Una **función o servicio** de salvaguarda no tiene una métrica propia, sino derivada de su poder reductor del Riesgo. El valor de la **Eficacia genérica** de una función o servicio de salvaguarda viene marcado por la experiencia de los analistas de seguridad y depende del tipo de dicha función o servicio de salvaguarda (o sea de su forma de actuación) y del tipo de Amenaza.

Los **mecanismos** de salvaguarda tienen una Métrica directamente ligada a su costo técnico u organizacional, traducido a pesos.

Para realizar esto es necesario contar con una lista de funciones o servicios de salvaguarda, organizadas por activo/amenaza, ordenadas por su efectividad.

2.5 ANÁLISIS COSTO BENEFICIO

La seguridad en cualquier sistema debe ser proporcional con sus riesgos. Sin embargo, el proceso para determinarse cual control de seguridad es apropiado y rentable, es a menudo bastante complejo y en ocasiones una cuestión subjetiva. Una de las funciones primeras del análisis del riesgo de la seguridad es poner este proceso sobre una base más objetiva.

En la práctica existen dos aproximaciones para responder a estas cuestiones, una cuantitativa y otra cualitativa.

2.5.1 Análisis de riesgos cuantitativo

Este acercamiento emplea dos elementos fundamentales; la probabilidad de ocurrencia de un acontecimiento y la pérdida probable si ocurre.

El análisis cuantitativo del riesgo hace uso de una sola figura producida de estos elementos. Esto se llama la ' expectativa anual de pérdida (ALE) ' o el ' costo anual estimado (EAC)'. Esto es calculado para un acontecimiento simplemente multiplicando la pérdida potencial por la probabilidad.

Es así teóricamente posible alinear acontecimientos en orden del riesgo (ALE) y tomar las decisiones basadas sobre esto.

Los problemas con este tipo de análisis del riesgo se asocian generalmente a la falta de fiabilidad y a la inexactitud de los datos. La probabilidad puede raramente ser exacta y puede, en algunos casos, promover la satisfacción personal. Además, los controles y las salvaguardas abordan a menudo un número de acontecimientos potenciales y los acontecimientos se correlacionan con frecuencia.

A pesar de las desventajas, un número de organizaciones ha adoptado con éxito el análisis de riesgos cuantitativo.

2.5.2 Análisis de riesgo cualitativo

Éste es por mucho el más usado para el análisis de riesgos. Los datos de la probabilidad no se requieren y solamente se utiliza la pérdida potencial estimada.

La mayoría de las metodologías cualitativas de análisis de riesgos hacen uso de un número de elementos relacionados:

Amenazas.
Éstas son las cosas que pueden ir mal o que pueden ' atacar ' el sistema. Los ejemplos pueden incluir el fuego o fraude. Las amenazas están siempre presentes para cada sistema.

Vulnerabilidades.
Este hace un sistema más propenso a un ataque por una amenaza o hace un ataque más probable de tener cierto éxito o impacto. Por ejemplo, por fuego una vulnerabilidad sería la presencia de materiales inflamables (ej. papel).

El Impacto.
Será cualitativo con pérdidas funcionales (de los estados de seguridad); cualitativo con pérdidas orgánicas (de fondo de comercio, daño de personas, etc.); y cuantitativo si las pérdidas se pueden traducir en dinero directa o indirectamente.

La primera de ellas es por mucho la menos usada, ya que en muchos casos implica cálculos complejos o datos difíciles de estimar. Se basa en dos parámetros fundamentales: la probabilidad de que un suceso ocurra y una estimación del costo o las pérdidas en caso de que así sea; el producto de ambos términos es lo que se denomina **costo anual estimado,** y aunque teóricamente es posible conocer el riesgo de cualquier evento y tomar decisiones en función de estos datos, en la práctica la inexactitud en la estimación o en el cálculo de parámetros hace difícil y poco realista este método.

El segundo método de análisis de riesgos es el cualitativo, de uso muy difundido en la actualidad especialmente entre las nuevas `consultoras' de seguridad (aquellas más especializadas en seguridad lógica, cortafuegos, pruebas de penetración y similares). Es mucho más sencillo e intuitivo que el anterior, ya que ahora no entran en juego probabilidades exactas sino simplemente una estimación de pérdidas potenciales.

Para ello sé interrelacionan cuatro elementos principales: las amenazas, por definición siempre presentes en cualquier sistema, las vulnerabilidades, que potencian el efecto de las amenazas, el impacto asociado a una amenaza, que indica los daños sobre un activo por la materialización de dicha amenaza, y los controles o salvaguardas, contramedidas para minimizar las vulnerabilidades (controles preventivos) o el impacto (controles curativos).

Por ejemplo, una amenaza sería un pirata que queramos o no (no depende de nosotros) va a tratar de modificar nuestra página *web* principal, el impacto sería una medida del daño que causaría si lo lograra, una vulnerabilidad sería una configuración incorrecta del servidor que ofrece las páginas, y un control la reconfiguración de dicho servidor o el incremento de su nivel de "parchado".
Con estos cuatro elementos podemos obtener un indicador cualitativo del nivel de riesgo asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

2.6 REEVALUAR EL RIESGO

Descripción y objetivo:

Se aplica las funciones y servicios de salvaguarda seleccionados a la reducción de la frecuencia de ocurrencia de la amenaza (disminución de la vulnerabilidad) y a la reducción del impacto.

Los nuevos niveles de vulnerabilidad y de impacto se identifican y estiman rehaciendo el procedimiento establecido por las Actividades de 'Identificación y estimación de vulnerabilidades' e 'Identificación y valoración de impactos' realizados ya en una ocasión.

Los nuevos niveles de vulnerabilidad y de impacto permiten calcular el *riesgo efectivo* aplicando la misma forma de evaluación del riesgo presentada anteriormente.

Este valor del riesgo efectivo calculado se ha de guardar, pues será el riesgo residual si en la actividad siguiente se alcanza el cumplimiento de objetivos del proyecto de Análisis y Administración de Riesgos.

2.6.1 Cumplimiento de objetivos

La actividad examinará si los riesgos efectivos obtenidos por la aplicación sucesiva de las funciones y servicios de salvaguarda seleccionados se encuentran bajo los umbrales de riesgo elegidos.

2.6.1.1 Determinar el cumplimiento de los objetivos

Descripción y objetivo:

Si los riesgos efectivos calculados en la tarea anterior no cumplen los objetivos de su reducción por debajo de los umbrales de riesgo fijados, la tarea implica

la conservación provisional de los resultados parciales alcanzados (puede haber ‘retrocesos’ en este proceso de simulación).

La repetición de toda la actividad de selección de las funciones y servicios de salvaguarda, o sea de las tareas de reconsiderar la selección y reevaluar el riesgo, antes de vover a comprobar el cumplimiento de los objetivos con esta tarea.

El Comité director debe aprobar el conjunto de funciones y servicios de salvaguarda propuestos.

La Dirección procederá a la aprobación o no de los resultados de la Etapa presentados por el Director del Proyecto.

2.7 RESULTADOS

2.7.1 Documentación intermedia

• Lista de funciones y servicios de salvaguarda ordenados según su efectividad, con una descripción de sus características.

• Informe de funciones y servicios de salvaguarda existentes, estimando su efectividad.

• Informe de funciones y servicios de salvaguarda seleccionados, con justificación de cada uno.

• Nuevos valores del riesgo al aplicar las funciones y servicios de salvaguarda propuestos.

• Informe del estudio comparativo de resultados en las simulaciones.

2.7.2 Documentación final

Lista final de funciones y servicios de salvaguarda propuestos.

2.7.3 Resumen

Los nuevos tipos de amenaza (sobre todo las intencionales sean locales o sean de origen remoto, es decir con necesidad de presencia física o sistema de telecomunicación) requieren nuevos tipos de salvaguarda. Se empieza a superar el modelo estático de protección, representado a menudo como en una 'fortaleza' cuyas 'brechas' o vulnerabilidades concretas de sus Activos deben impermeabilizarse con salvaguardas específicas.

Los resultados de esta evaluación ayudarán a orientar y a determinar las prioridades y acciones de administración adecuadas para la administración de los riesgos concernientes a seguridad de la información, y para la implementación de los controles seleccionados a fin de brindar protección contra dichos riesgos.

Puede resultar necesario que el proceso de evaluación de riesgos y selección de controles deba llevarse acabo en varios ciclos, a fin de cubrir diferentes partes de la organización o sistemas de información individuales.

Es importante llevar a cabo revisiones periódicas de los riesgos de seguridad y de los controles implementados a fin de:

d) Reflejar los cambios en los requerimientos y prioridades de la empresa.
e) Considerar nuevas amenazas y vulnerabilidades.
f) Corroborar que los controles siguen siendo eficaces y apropiados.

Las revisiones deben llevarse a cabo continuamente dejando como máximo entre una revisión y otra 6 meses, con diferentes niveles de profundidad según los resultados de evaluaciones anteriores y los niveles variables de riesgo que la gerencia está dispuesta a aceptar.

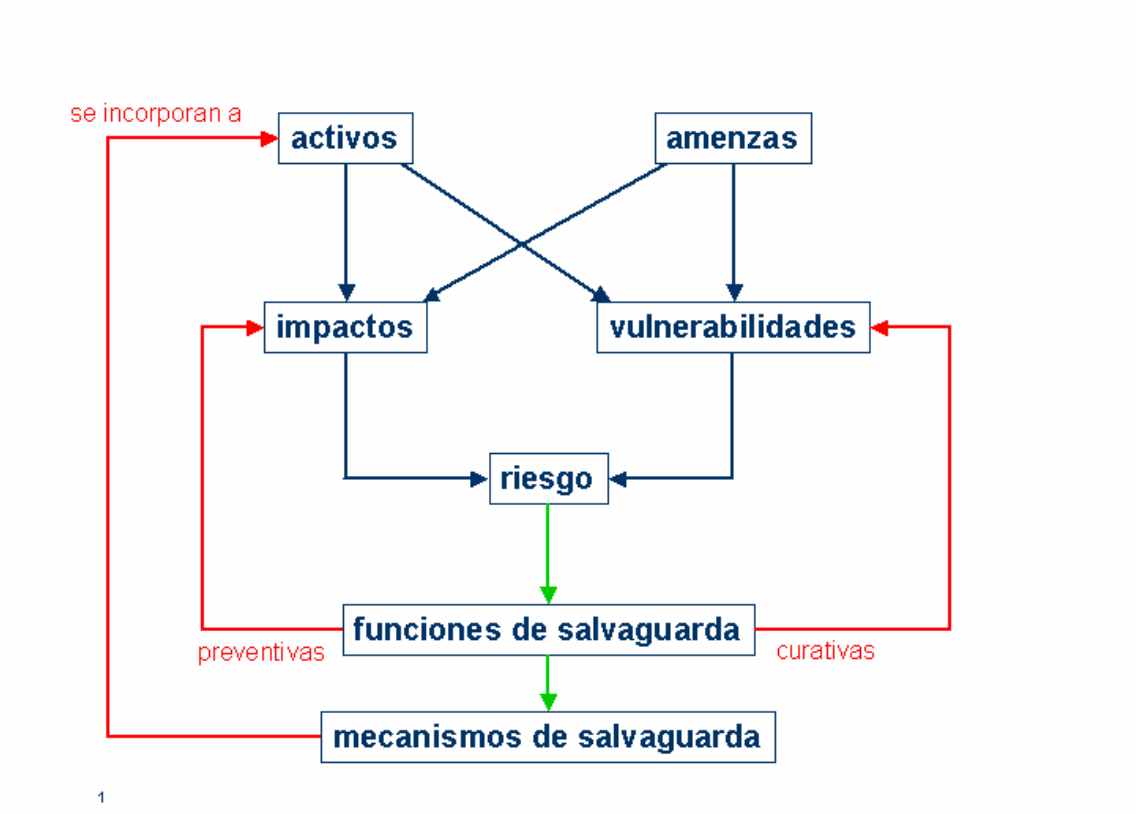

Figura 2.
[8] Guía de procedimientos.

Esta imagen representa la relación entre el análisis de riesgo y la administración de riesgos, en él capitulo 1. de esta tesis únicamente se estudiaron los cinco primeros puntos: Activos, amenazas, vulnerabilidades, impactos, y riesgos; En este segundo capitulo se estudian los puntos restantes: funciones y mecanismos de salvaguarda.

3 POLÍTICAS DE SEGURIDAD INFORMÁTICA

3.1 Introducción

Actualmente la seguridad informática ha tomado gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para explorar más allá de las fronteras nacionales, situación que ha llevado a la aparición de nuevas amenazas en los sistemas informáticos. [9]

Esto ha llevado a que muchas organizaciones gubernamentales y no gubernamentales internacionales hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

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

Las buenas prácticas de administración indican que la existencia de un enunciado público claro de una misión de una organización es indispensable para que todos los miembros ubiquen sus propios esfuerzos.

Se evitan confusiones y alegatos, se fomenta la productividad y se logra un mejor ambiente de trabajo, permite elaborar políticas operativas que facilitan el cumplimiento de la misión de la organización, que deben entenderse como reglas que hay que seguir obligatoriamente.

Casi siempre se enuncian en forma positiva, indican que debe hacerse y en ocasiones como, aunque también en forma negativa como prohibiciones. [4]

Una Política de Seguridad es el conjunto de lineamientos que regirá el buen uso de los recursos informáticos y de cómputo de una Organización. Refleja los principales objetivos de la Organización. En ella se describen tanto los derechos como las obligaciones a que están sujetos los diferentes tipos de usuarios.

Estos lineamientos deben estar en acorde con las normas que rigen a la Organización, tanto internas como externas (o de carácter jurídico), así como de un análisis de riesgos sobre los activos de la misma.

No hay recetas mágicas, cada organización, dependiendo de su giro y de su entorno, deberá diseñar su propia Política de Seguridad.

3.1.2 Misión de seguridad

Es el enunciado de las aspiraciones que tienen los miembros de una organización en seguridad con respecto al uso de la tecnología informática.

Concebir y redactar la misión y las políticas de una organización recae sobre los responsables del buen funcionamiento de la misma. ***Por ejemplo los dueños de una empresa, los principales administradores de una corporación o los directores de alguna dependencia según sea el caso.*** El elemento fundamental de estos documentos es que expresan el consenso de quienes conocen mejor que nadie los principios operativos, económicos y éticos que conducirán al éxito colectivo. [4]

Al hacer este trabajo es necesario consultar a los expertos en diversos tipos de actividades, con la finalidad de que los directivos sepan como afectaran las políticas que emitan la capacidad de acción de las diferentes áreas de la organización. La forma más eficiente de realizar ésta consulta *es mediante una encuesta preparada por expertos en Seguridad Informática* que planteen las preguntas en forma tal que conduzcan a párrafos precisos en la redacción de la misión, cada uno de los cuales pueda plasmarse en una o más políticas de seguridad.

Todas las áreas de seguridad trabajan de manera conjunta para establecer una infraestructura de seguridad que sirva a toda la organización. Define que comportamiento es aceptable y cuales son los riesgos aceptables, y determina como se mitigan los riesgos que no son aceptables aplicando garantías que hacen manejables y aceptables los riesgos.

3.1.3 Errores mas frecuentes

Un grupo de personas dedicadas a la seguridad informática miembros del SANSI (System Administration, Networking and Security Institute), consideran que los errores más frecuentes que cometen los directivos son:

1. Suponer que los problemas desaparecerán si no se les hace caso.

2. Autorizar soluciones reactivas y parches de corto plazo tales que los problemas reaparecen rápidamente.

3. No entender cuanto dinero vale la información y que tanto depende de ella la reputación corporativa.

4. Depender principalmente de un firewall (cortafuegos).

5. No lidiar con los aspectos operacionales de la seguridad: Hacer sólo unos cuantos parches y no dar seguimiento para estar seguros de que los problemas en verdad estén resueltos.

6. No entender la relación que existe entre la seguridad y los problemas de funcionamiento. Entienden la seguridad física pero no ven las consecuencias de una mala seguridad informática.

7. Designan a personas no capacitadas para mantener la seguridad y no las capacitan ni les dan tiempo para capacitarse.

Es importante mencionar estos puntos en esta parte del capitulo dado que esta parte es realmente importante para poder implementar una seguridad informática adecuada y poder asegurar su éxito, ya que esta directamente vinculada con la alta dirección de cualquier empresa.

3.1.4 Consenso

No existe una formula para encontrar las mejores palabras que expresen la intención colectiva de una organización. La puede redactar una sola persona o emerger después de una sesión colectiva de intercambio de opiniones, o se puede tomar de algún documento establecido y adecuarlo a las necesidades de la organización.

Las organizaciones empresariales tienen como objetivo tanto obtener los mayores beneficios económicos como ser capaces de existir durante el máximo tiempo posible. Para ello realizan un plan estratégico en el que se reflejan cuáles son las líneas productivas que se deben seguir manteniendo, cuáles deberían implantarse y qué modificaciones debe sufrir la organización para lograr sus objetivos.

Se recomienda que se emplee tiempo de los directivos en un retiro, para discutir las preguntas buscando temas en los que exista consenso, durante la discusión pueden aparecen sutilezas, cambios en el entorno y los participantes más experimentados pueden compartir su punto de vista a los más inexpertos.

3.2 MÉTODO DELPHI

El método Delphi es un mecanismo para explorar las vías hacia el consenso, que se emplea rutinariamente en grupos colegiados y legislativos, y que consiste en términos generales de rondas de preguntas o propuesta presentadas al cuerpo deliberativo en forma tal que sus respuestas no se puedan discutir abiertamente, solamente en forma acotada y encauzada. Existen muchas variantes de este método[4].

Consiste en interrogar individualmente, por medio de una serie de cuestionarios, a un panel de "expertos" seleccionados en función de su profesión, cultura o cargo, con el objetivo de identificar escenarios futuros en los temas de interés.

Las discusiones colectivas tienden a ser dominadas por uno o dos individuos y tienden a apegarse a una sola idea durante periodos largos.

3.2.1 Definición

Es un método para estructurar el proceso de comunicación de un grupo de personas para que funciones efectivamente lidiando con problemas complejos. Los participantes son los que deciden: él o los individuos qué esperan obtener el producto del ejercicio Delphi para sus propósitos.

Se emplean modeladores: quienes diseñan los cuestionarios, resumen los resultados y conducen el proceso para satisfacer los requerimientos de quienes deciden. Se acude a expertos cuya opinión se necesita y a quienes se les hacen preguntas.

3.2.2 Metodología

- Los moderadores preparan una serie de preguntas para los expertos.

- Se solicita y evalúa su opinión sin que se comunique entre ellos.

- Se prepara una segunda serie de preguntas.

- Se solicita y se evalúa su opinión sin que se comunique entre ellos.

Y así sucesivamente hasta lograr el consenso o encontrar bloques donde el consenso sea imposible.

3.2.3 Características

El método Delphi pretende extraer y maximizar las ventajas que presentan los métodos basados en grupos de expertos y minimizar sus inconvenientes. Para ello se aprovecha la sinergia del debate en el grupo y se eliminan las interacciones sociales indeseables que existen dentro de todo grupo. De esta forma se espera obtener un consenso lo más fiable posible del grupo de expertos [17].

Este método presenta tres características fundamentales:

- **Anonimato:** Durante un Delphi, ningún experto conoce la identidad de los otros que componen el grupo de debate. Esto tiene una serie de aspectos positivos, como son:

    - Impide la posibilidad de que un miembro del grupo sea influenciado por la reputación de otro de los miembros o por el peso que supone oponerse a la mayoría. La única influencia posible es la de la congruencia de los argumentos.

    - Permite que un miembro pueda cambiar sus opiniones sin que eso suponga una pérdida de imagen.

- El experto puede defender sus argumentos con la tranquilidad que da saber que en caso de que sean erróneos, su equivocación no va a ser conocida por los otros expertos.

- **Iteración y realimentación controlada:** La iteración se consigue al presentar varias veces el mismo cuestionario. Como, además, se van presentando los resultados obtenidos con los cuestionarios anteriores, se consigue que los expertos vayan conociendo los distintos puntos de vista y puedan ir modificando su opinión si los argumentos presentados les parecen más apropiados que los suyos.

- **Respuesta del grupo en forma estadística:** La información que se presenta a los expertos no es sólo el punto de vista de la mayoría, sino que se presentan todas las opiniones indicando el grado de acuerdo que se ha obtenido.

3.2.4 Procedimiento

La misión debe redactarse en varios párrafos, cada uno de los cuales contendrá una colección de conceptos relacionados, susceptibles de ser rechazados conjuntamente.

Cada párrafo se escribe en una hoja de papel. Cada uno de los conceptos debe ser susceptible de plasmarse en una o más políticas de seguridad. Este material es preparado por los moderadores de la sesión Delphi, con la ayuda de especialistas en seguridad informática que hayan tenido la oportunidad de estudiar la organización.

Los participantes serán los miembros del organismo normativo. Cada participante anotar en su hoja un número que indicará su total acuerdo con un 10 junto con el párrafo, o su desacuerdo total con un 0, pudiéndose anotar un indicador de acuerdo parcial. Se recogerán de inmediato las hojas mencionadas. Se repetirá este proceso para todos los párrafos que constituyen la misión.

Primera Ronda*:* por medio de los cuestionarios se pide a los panelistas que pronostiquen las tendencias o eventos relativos a las áreas de interés. Las respuestas son procesadas estadísticamente buscando tanto el "centro" de la opinión grupal como las posturas que se desvían de ese centro.

Segunda Ronda: a aquellos panelistas cuyas respuestas o consideraciones prospectivas se alejen de la zona de concentración mayoritaria se les pregunta nuevamente, adicionando en el formulario los argumentos más consensados por el resto del panel para que les sea posible reconsiderar su posición anterior.

El procedimiento mediante rondas se repite hasta llegar a consensos o acuerdos generales sobre la evolución futura de los temas de interés.

El resultado final de la secuencia Delphi está dado por el conjunto de los pronósticos más reiterados, eventualmente acompañados de medidas de dispersión de las respuestas, y un resumen de insumos críticos y argumentos relacionados con cada evento pronosticado.

3.2.5 Métrica

Para cada párrafo se calculará el promedio y dispersión de las medidas de aceptación:

- Los que obtengan una aceptación de 8 ó mayor, con una dispersión baja se consideran aceptados.

- Los que obtengan una aceptación de 2 ó menor, con una dispersión baja se consideran rechazados.

- Los que obtengan una aceptación entre 2.1 y 7.9, y los que tengan una aceptación con una dispersión alta se someterán a una nueva evaluación.

Para cada párrafo a evaluar en la segunda ronda, se entrega a los participantes una hoja en la que aparezca el párrafo a evaluar y se invita a un voluntario a hablar a favor, y otro que hable en contra. Al terminar los argumentos se procede a recoger las evaluaciones. Se repite el proceso con todos los demás párrafos de la segunda ronda.

Al terminar la segunda ronda se clasifican los párrafos como aceptados o rechazados, los párrafos aceptados constituyen la misión de seguridad y dan origen a las políticas que deben adoptarse y a los mecanismos que se implanten.

3.2.6 Participantes

Los actores participantes en las políticas de seguridad y sus responsabilidades son:

Alta administración.

- Tiene la responsabilidad del éxito de la organización.
- Fija los objetivos, metas y prioridades para apoyar la misión de la organización.
- Verificar que se asignen recursos adecuados al programa y que este se desarrolle con éxito.
- Dar el ejemplo a los demás.

Dueños de programas, administradores de funciones, dueños de aplicaciones.

- Aplican medidas de seguridad a sus áreas de responsabilidad.
- Aplican controles técnicos, administrativos y operativos.
- Sus subordinados son los que hacen el verdadero trabajo directo.

Administradores de la seguridad de sistemas de cómputo.

- Guían la administración diaria del programa de seguridad en cómputo.
- Coordinan las interacciones que involucran la seguridad de los diversos elementos externos de la organización.
- Frecuentemente, si los programas, funciones, o aplicaciones son grandes o complicadas, se asigna a cada una un oficial de seguridad.

Administradores de configuraciones, proveedores de tecnología.

- Implementan la tecnología de seguridad diseñada para el sistema.
- Deben dar continuidad a sus sistemas.
- Probablemente pertenezcan a una organización grande de administración de recursos de información.
- Pueden atender incidentes directamente.
- Organizaciones de soporte.
- Analizan la vulnerabilidad de los sistemas.
- Proveen los servicios de comunicación.
- Ayudan a los dueños y administradores a implantar y vigilar sistemas específicos para u programa o aplicación.
- Coordinan los sistemas de seguridad entre aplicaciones o programas.

Auditores, especialistas en seguridad física, especialistas en planes de contingencia, especialistas en recuperación después de desastres, especialistas en calidad y confiabilidad, departamento de adquisiciones y soporte, departamento de capacitación, departamento de personal, especialistas en administración de riesgos, departamento de servicios generales, verificadores independientes, equipos de penetración independientes, usuarios de sistemas.

- Acatar las disposiciones de seguridad.
- Reportar problemas de seguridad.
- Acudir a las instancias de capacitación.

3.3 ¿QUÉ SON LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA?

Objetivo: proporcionar dirección y apoyo gerencial para brindar seguridad de la información. El nivel gerencial debe establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una política de seguridad de la información através de toda la organización. [5]

Una vez que se ha establecido la misión de seguridad informática se requiere redactar las políticas de seguridad informática en que se basará el cumplimiento de la misión.

Se mostrarán diferentes tipos de definiciones de políticas de seguridad informática, algunas son más especificas que otras.

Podemos entender como políticas de seguridad, el conjunto de reglas y principios que rigen una entidad u organismo, donde cada regla define una acción, mecanismo y/o procedimiento.

Entre las características más relevantes a considerar durante su definición son:
- Enfoque a la problemática particular de cada organización.
- Contar con una estructura bien definida.
- Vigencia y flexibilidad para su actualización.
- Que establezca obligaciones y derechos.
- Que sean aprobadas y difundidas por los directivos, administradores y usuarios de la organización.

De tal forma que se pueda contar con un documento de políticas de seguridad informática que sirva de guía en caso de violaciones a la seguridad y que sirvan de apoyo para ir a la par de la tecnología cubriendo la falta de legislación.[12]

Una política de seguridad es una declaración formal de las reglas, las cuales la gente que tenga acceso a los activos de la tecnología y de la información de una organización debe seguir.[13]

[10]Políticas de seguridad son los documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos que tanto usuarios como administradores tienen y qué hacer ante un incidente de seguridad.

Son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de daño sobre: las computadoras de sus sistemas y los elementos físicos asociados con éstos (edificios, impresoras, discos, cables, dispositivos de interconexión, etc.), el software y la información almacenada en tales sistemas, los usuarios del sistema, etc. [11]

Mientras las políticas indican el “qué”, los procedimientos indican el “cómo”. Los procedimientos son los que nos permiten llevar a cabo las políticas.
Ejemplos que requieren la creación de un procedimiento son:

- Otorgar una cuenta.
- Dar de alta a un usuario.
- Conectar una computadora a la red.
- Localizar una computadora.
- Actualizar el sistema operativo.
- Instalar software localmente o vía red.
- Actualizar software crítico.
- Exportar sistemas de archivos.
- Respaldar y restaurar información.
- Manejar un incidente de seguridad.

Para que esto sirva de algo, las políticas deben ser:

- Apoyadas por los directivos.
- Únicas.
- Claras (explícitas).
- Concisas (breves).
- Bien estructuradas.
- Servir de referencia.
- Escritas.
- Revisadas por abogados.
- Dadas a conocer.
- Entendidas por los usuarios.
- Firmadas por los usuarios.
- Mantenerse actualizadas.

Las políticas son parte fundamental de cualquier esquema de seguridad eficiente. Como administradores, nos aminoran los riesgos, y nos permiten actuar de manera rápida y acertada en caso de haber una emergencia de cómputo. Como usuarios, nos indican la manera adecuada de usar un sistema, indicando lo que puede hacerse y lo que debe evitarse en un sistema de cómputo, contribuyendo a que no seamos “malos usuario” de la red sin saberlo. El tener un esquema de políticas facilita en gran manera la introducción de nuevo personal, teniendo ya una base escrita y clara para capacitación; dan una imagen profesional a la organización y facilitan una auditoria.

Los principales puntos que deben contener las políticas de seguridad son:

- Ámbito de aplicación.
- Análisis de riesgos.
- Enunciados de políticas.
- Sanciones.
- Sección de uso ético de los recursos de cómputo.
- Sección de procedimientos para el manejo de incidentes.

Al diseñar un esquema de políticas de seguridad, conviene que dividamos nuestro trabajo en varias y diferentes políticas específicas a un campo o área en concreto como podría ser: cuentas, contraseñas, control de acceso, uso adecuado, respaldos, correo electrónico, contabilidad del sistema, seguridad física, personal, etc.

Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes. Las políticas de seguridad informática establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización.

No es una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y el por qué de ello.

Cada política de seguridad informática es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

3.3.1 Definición de una política de seguridad

[12]Cuando en una organización surge la iniciativa de generar sus propias políticas de seguridad, puede enfrentarse a un gran número de interrogantes, como:

¿Quiénes son los responsables de desarrollar las políticas?

¿Quiénes deben de darle la importancia requerida?

¿Que deben de abarcar?

¿Que características deben tener?

¿Cómo hacerlas cumplir?

Por ello, el proceso de definición de políticas que aquí se presenta abarca las siguientes etapas:

Planeación y preparación, desarrollo, aprobación, difusión y aplicación, revisión y actualización.

3.3.2 Planeación

Desde la etapa de **planeación** de las políticas, ***es necesario contar con el apoyo del cuerpo directivo de la organización en cuanto a la definición de las mismas.*** Y conocer la postura institucional en cuanto a la política de seguridad informática general que deberá seguirse durante el **desarrollo** de las políticas de seguridad particulares.

También es importante, ***detectar la problemática de la organización através de un análisis de riesgos***, definir lo que se debe proteger, así como informarse acerca de la legislación en el país o entidad en donde se aplique.

3.3.3 Desarrollo

Para iniciar su **desarrollo**, es importante contar con una persona que sea responsable de dar seguimiento al proceso de definición de las políticas y de darle continuación al proceso cuando sea detenido, normalmente se le nombra coordinador.

3.3.4 Redacción

En la **redacción** de las políticas en necesaria la participación de los administradores de sistemas de cómputo; una persona que represente al cuerpo directivo, el encargado de guiar el desarrollo de las mismas de acuerdo a la política institucional en cuanto a la seguridad de sus activos, un asesor jurídico que vigile que en la redacción de las políticas no se violen las garantías individuales de los usuarios y que estén de acuerdo con la actual legislación en el área de aplicación, y algunos usuarios de la red que aporten información sobre los usos de la tecnología en sus actividades, de tal manera que los servicios críticos para la actividad de la organización no se vean afectados sino protegidos.

Entre las principales características a considerar para el documento de políticas durante su desarrollo, se encuentran:

1.- Enfocar la política hacia la problemática particular de la organización.
2.- Contar con un documento con una estructura bien definida.
3.- Definición clara y precisa de los enunciados.
4.- Que exponga de manera explícita el ámbito de aplicación.
5.- Que se establezcan obligaciones y derechos tanto para los administradores como para los usuarios.
6.- Que defina claramente las sanciones a las que estará sujeto quién no se apegue a las políticas de seguridad institucionales.
7.- Que el documento cuente con vigencia y flexibilidad para su actualización.

3.3.5 Aprobación

Una vez concluida la redacción de las políticas, se procede con su **aprobación**.

Esta etapa consiste normalmente de una revisión final exhaustiva por parte del cuerpo directivo de la organización, hasta su **aprobación**. ***En algunos casos el tiempo de elaboración del documento en esta etapa es largo, ya que dependerá en cierta forma de la disposición y prioridad del documento ante los directivos***. De allí que es indispensable vender la idea desde su planeación.

3.3.6 Difusión y aplicación

La **difusión y aplicación** de políticas es el siguiente paso, es de vital importancia difundir el documento através de diversos medios como, pagina principal de la organización, correo electrónico, trípticos, en la apertura de cuentas a nuevos usuarios, publicación en revistas internas electrónicas y tradicionales, etc. De tal forma que sea conocido por todos los usuarios de la organización, y que sea transparente su aplicación y seguimiento.

Las políticas deben ser **aplicadas** tanto por los *directivos* como por los *administradores* y *los usuarios*, ya que la seguridad no depende de una sola persona sino de cada uno de los individuos que forman una organización.

El proceso de definición de políticas de seguridad es continuo aún después de ser aprobadas, difundidas y aplicadas, ya que su siguiente etapa es la de revisión y actualización de acuerdo a la naturaleza cambiante de las tecnologías de la información.

3.3.7 Fortalezas

La política de seguridad como se ha definido antes, es creada de forma explícita para un sistema según sus características como misión, recurso, tipo de red y de usuarios, etc. De tal forma que, la Institución puede crear un mecanismo de control al crear la política de seguridad apropiada a sus necesidades, a voluntad y apegada a sus reglamentos administrativos y técnicos para definir el buen uso de sus recursos y como apoyo a posteriores procedimientos legales en dado caso.

Una fortaleza es un elemento que favorece de forma sustantiva el desempeño en este caso de un sistema de computo y comunicaciones de una institución. Al invertir en una política de seguridad se obtienen fortalezas como las siguientes:

1.- Uso definido de los recursos, es común entre las organizaciones adquirir recursos e iniciar su funcionamiento sin una definición escrita y sin divulgación entre sus usuarios sobre el tipo de servicio que brindará y sus restricciones.

2.- Derechos y obligaciones definidas para cada tipo de usuario, es importante definir y difundir esa información entre todos los usuarios del sistema, de tal forma que cada usuario conozca sus alcances y limitaciones sobre los recursos.

3.- Guías técnicas para la protección de recursos, información de gran utilidad para los usuarios, la seguridad es una responsabilidad compartida entre todos los usuarios de un sistema, son tan importantes las técnicas locales(contraseña de un usuario) como las técnicas aplicadas a niveles globales(firewalls). La institución elige las herramientas más apropiadas para sus recursos y separar el conocimiento para su aplicación por todos.

4.- Análisis de riesgos sobre inventarios de recursos, es común la falta de estudios de este tipo, siendo de gran relevancia para el desarrollo mismo de las políticas y el conocimiento de las debilidades del sistema. Esta información define la diversidad de riesgos y propone la prioridad y el nivel de protección de los recursos; elementos que son necesarios para la generación de planes de contingencia.

5.- Sanciones definidas dentro del marco ejecutivo de la institución, en caso de mal uso de los recursos, la institución tendrá una herramienta para aplicar las sanciones apropiadas sobre un marco de reglas locales y conocidas por todos. Es importante mencionar que las sanciones definidas en una política de seguridad no pueden estar en contra de las leyes estatales y/o federales, las políticas son un apoyo a la falta de legislación, de ninguna manera pueden contradecirla.

6.- Planes de contingencia, dentro del documento de las políticas se encuentran enunciados todos los planes de contingencia generados para el sistema.

7.- Pueden modificarse cuando sea necesario, las políticas deben crecer con la institución, ajustarse tanto a los cambios internos como a los cambios en la ley gubernamental. Los cambios los propone un comité o grupo de seguridad en respuesta a elementos nuevos o cambios importante(técnicos o administrativos) y éste decide cuándo y cómo cambiarlas para mantener su actualidad.

8.- Un documento firmado por directivos y que es la ley dentro de la institución, las políticas pueden ser el marco de referencia de todos en un sistema, para practicar buenos hábitos, contribuir al desarrollo optimo de la institución, aportar para fortalecer la cultura informática en la institución. Un documento que apoye a la institución dentro de su dominio a falta de legislación informática en el marco jurídico.

3.3.8 Beneficios

Las políticas de seguridad informática normalmente ayudan a tomar decisiones sobre otros tipos de política. También son útiles al tomar decisiones sobre nuevas adquisiciones, ya que algunos equipos o programas no serán aceptables en términos de las políticas mientras otros la sustentan.

Si ocurre un incidente las políticas constituyen un marco de referencia sobre quién tiene autoridad para tomar acciones que minimicen el impacto del incidente y sobre que acciones hay que tomar para que no se repita un incidente similar. Permiten identificar y castigar a quienes resulten responsables.

Se deben considerar como un documento de largo plazo, va evolucionando. No contiene asuntos específicos de implementación pero sí asuntos específicos de los sistemas de tecnologías de la información de la organización.

El diseño e implementación de las políticas de seguridad informática, es una indicación de que una organización esta bien administrada, y los auditores lo toman en cuenta en sus evaluaciones. Conducen a una profesionalización de la organización.[4].

3.4 ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA

3.4.1 CRITERIOS DE LA OCDE

La OCDE es la organización para la cooperación y el desarrollo económico, considera que los elementos de las políticas son:

- La responsabilidad de los administradores, proveedores, y usuarios de información debe hacerse explícita (responsabilización).

- Los administradores, proveedores y usuarios de información deben tener conciencia de la existencia y dimensión de las medidas de seguridad (concientización).

- Los servicios de información y su seguridad deben prestarse en forma ética (ética).

- Los esquemas de seguridad deben adoptar un enfoque multidisciplinario (multidisciplinareidad).

- Los niveles, costos, medidas, prácticas y procedimientos deben ser apropiados y proporcionales al valor de la información y a la probabilidad de ataques severos (proporcionalidad).

- Los procedimientos, medidas y prácticas de seguridad de la información debe coordinarse e integrarse con los procedimientos, medidas y prácticas de seguridad de la organización para establecer un sistema coherente. (Integración).

- Los usuarios públicos y privados en el ámbito nacional e internacional deben funcionar en forma coordinada y oportuna para prevenir y responder a violaciones de la seguridad de sistemas de información (oportunidad).

- Los sistemas de seguridad de la información deben reevaluarse periódicamente (reevaluación).

- Los sistemas de seguridad de la información deben ser compatibles con el uso y flujo legitimo de la información en una sociedad democrática (democracia).

Como se dijo anteriormente, una Política de seguridad informática debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere una disposición de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

3.4.2 Posturas

En las políticas de seguridad hay que analizar las actividades que se desarrollan en el ambiente de tecnologías de la información y pronunciarse sobre su aceptabilidad. Para aclarar las ideas, se pueden considerar dos extremos:

Todo lo que no está explícitamente permitido está prohibido.

Todo lo que no está explícitamente prohibido está permitido.

El segundo enunciado es más fácil de implementar y resulta eficiente en algunos casos sencillos, posiblemente para empresas pequeñas, pero no proporciona una seguridad robusta. El primero requiere de conocimientos amplios del funcionamiento de los sistemas y de mucho más trabajo al inicio y

bastante trabajo de mantenimiento, y como consecuencia nos proporciona una seguridad robusta.

Las Política de seguridad informática deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y de las consecuencias del in cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que se tenga acceso.

Las Política de Seguridad Informática deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones, transmitir por qué son importantes éstos u otros recursos o servicios.

De igual forma, las Política de Seguridad Informática establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía.
Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otro lado, la política de debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud que pasará cuando algo suceda; no es una sentencia obligatoria de la ley.

Las Política de Seguridad Informática como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

3.4.3 Algunos parámetros para establecer Políticas de Seguridad

Si bien las características de las políticas de seguridad informática que hemos mencionado hasta el momento, nos muestran una perspectiva de las implicaciones en la formulación de estas directrices, revisemos algunos aspectos generales recomendados para la formulación de las mismas.

- Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las políticas de seguridad informática de su organización.

- Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a las políticas de seguridad informática.

- Comunique a todo el personal involucrado en el desarrollo de las políticas de seguridad informática, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los interesados en salvaguardar los activos críticos de la funcionalidad de su área u organización.

- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas

- Un consejo más, no dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las políticas de seguridad informática trazadas.

3.5 PROCESO DEL DISEÑO DE POLÍTICAS

Las decisiones unipersonales acerca de las políticas de seguridad tienden a estar sesgadas por la experiencia y la visión de las empresas. Por esta razón es mucho mejor designar a un equipo que se encargue del diseño de las políticas.

Anteriormente se definieron algunos puntos importantes, ahora trataremos de especificarlas un poco más.

Ya que es muy extenso el campo de aplicación de las políticas de seguridad informática, desde que se inicia este proceso hay que especificar el alcance de las políticas y los objetivos de los mismos, consistencia con la misión de seguridad previamente establecida.

Las políticas promulgadas deben escribirse en secciones o párrafos que sean, cada uno por separado, que se puedan implementar mediante un mecanismo especifico. Hay que procurar que pensar claramente en la conveniencia de que las políticas sean sumamente especificas, esta fragmentación facilita su mantenimiento. También es deseable fragmentar las políticas por departamento o unidad de trabajo.

Las políticas que no cuenten con la aceptación de todos los usuarios a todos los niveles serán muy difíciles de implantar, todas las personas a las que las políticas afecten deben tener la oportunidad de revisarlas y hacer comentarios antes de que se promulguen. Pueden llegar a pensar que las políticas serán difíciles de implementar e incluso temerán un en exceso de controles, por lo cual se debe contar con el apoyo total de los administradores.

En esta etapa deben considerarse los mecanismos de difusión, capacitación y concientización iniciales y permanentes sobre seguridad informática. La cultura de la organización y sus necesidades de seguridad serán un factor determinante para el equipo de redacción de las políticas.

Las razones que llevan a la implantación de las políticas deben explicarse dentro de la política misma, junto con las demás características ya mencionadas. La resolución de dudas, conflictos de interés y tratamiento de las violaciones son temas que forman parte de las políticas de seguridad.

3.5.1 Algunas políticas necesarias

3.5.1.1 Políticas de uso aceptable

- Determinan qué se puede hacer con los recursos de cómputo de la organización.

- También determinan lo que no se puede hacer con esos recursos. Indica la responsabilidad de la protección de la información que maneja y en que condiciones pueden afectar leer datos que no les pertenezcan.

- Deben indicar si esta permitido compartir cuentas de usuario, como se debe usar el correo electrónico, los grupos de noticias y las paginas que hay en la red.

- Deben reflejar las políticas respeto y protección de la propiedad intelectual que tenga la organización aplicándolas a los programas de cómputo que se empleen.

- Todas las personas que utilicen las instalaciones de la empresa donde apliquen las políticas de seguridad deben leer y firmar su aceptación antes de tener acceso a los recursos.

3.5.1.2 Políticas de cuentas de usuario

Determinan el procedimiento que hay que seguir para adquirir privilegios de usuario en uno o más sistemas de información así como derechos y obligaciones.

También quien tiene la autoridad para dar esos privilegios, y quienes no podrían recibir esos privilegios por causas legales.

Debe explicar cómo y cuándo se deshabilitarán las cuentas de usuario y que se hará con la información que contenga.

Debe especificar claramente los detalles de los procedimientos de identificación y autenticación.

3.5.1.3 Políticas de acceso remoto

Se definen y explican los métodos aceptables para conectarse a los sistemas de información de la organización desde el exterior de la misma.

Son particularmente importantes para organizaciones geográficamente extendidas o aquellas cuyos miembros pasan la mayor parte del tiempo viajando.

También establece quien tiene derecho a este tipo de conexión, así como establecer quien puede emplear módems para conectarse al exterior de la organización, sobre todo módems de alta velocidad.

3.5.1.4 Políticas de protección de la información

El objetivo es que la información no sufra modificaciones ó sea difundida durante su proceso, almacenamiento, transmisión, etc.

Especifica como deben establecerse las jerarquías de confidencialidad e integridad, y cómo se implementa su protección.

Debe ponerse especial atención a la divulgación y destrucción de la información.

3.5.1.5 Políticas de configuración de cortafuegos

Establece quien determina el establecimiento y los cambios a la configuración.

Quien debe tener acceso a ser usuario del cortafuegos y quien puede obtener información acerca de la configuración del mismo.

Debe establecer ciclos de administración de la configuración para que responda a las necesidades de la organización.

3.5.1.6 Políticas de cuentas privilegiadas

- Establece los requisitos que deben satisfacer quienes usen cuentas privilegiadas, con respecto a su desempeño y trayectoria dentro de la organización.

- Contiene procedimientos de auditoría del uso de este tipo de cuentas, particularmente sobre los procedimientos y identificación y autenticación, y su uso.

- Determina en que condiciones se debe cancelar el acceso privilegiado.

3.5.1.7 Políticas de conexión a la red

- Define los requisitos que deben cumplirse para que se conecten nuevos dispositivos a la red de la organización.

- Son particularmente importantes para organizaciones que tienen una diversidad en equipos de soporte técnico, y para aquellos que no están protegidos por un cortafuegos.

- Deben especificar quien puede instalar nuevos recursos en la red, cuál es la autorización requerida y cómo se documentan los cambios.

- Deben aclarar como se manejan los dispositivos inseguros.

3.5.1.8 Restricciones a las políticas

La principal fuente de restricciones es la pérdida de productividad, es imposible evitar que la implementación de políticas de seguridad informática distraigan recursos humanos e informáticos que podían ser empleados en otros procesos. Si se coloca este problema en dos extremos, uno seria si nadie tiene acceso a la información, esta estará muy segura, pero nadie podría realizar su trabajo.
En el otro extremo si no se destinan recursos a tareas de seguridad, todos los recursos estarán dedicados a sus fines productivos, pero la información estará totalmente insegura.[4]

En una organización donde lo primordial son los resultados, el segundo extremo podría ser el más atractivo, y sus políticas reflejarán esta actitud, con los riegos que genera.
En una organización orientada a la sobre vivencia a largo plazo y al crecimiento estable, y sobre todo a tener actividades que se pueden replicar una y otra vez, se implementaran políticas más restrictivas.

Otra fuente de restricciones son: la legislación y los derechos de los empleados y de los clientes, en cada país existe una cultura diferente, así como cada organización tiene la suya propia.

3.5.2 ¿Porqué las Políticas de Seguridad Informática generalmente no se logran implantar?

Muchas veces las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito.

Según algunos estudios resulta una labor ardua el convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y la falta de una estrategia de mercado de los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para los

juguetes de los ingenieros". Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad, que en muchos de los casos lleva a comprometer su información sensible y por consecuencia su imagen corporativa.

Ante esta encrucijada, los encargados de la seguridad deben asegurarse de que las personas relevantes entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

En particular, la gente debe saber las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir. Una buena intrusión o una travesura puede convertir a las personas que no lo entendieron, en blanco de las políticas o en señuelos de los verdaderos vándalos.

Luego, para que las Políticas de Seguridad Informática logren abrirse espacio al interior de una organización *deben integrarse a las estrategias del negocio, a su misión y visión,* con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía. De igual forma, las políticas de seguridad informática deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en su diario hacer, donde se identifiquen las necesidades y acciones que materializan las políticas.

En este contexto, entender la organización, sus elementos culturales y comportamientos nos deben llevar a reconocer las pautas de seguridad necesarias y suficientes que aseguren la confiabilidad en las operaciones y funcionalidad de la compañía.

A continuación se dan algunas recomendaciones para vender las preocupaciones sobre la seguridad informática:

- Desarrolle ejemplos organizacionales relacionados con fallas de seguridad que capten la atención de sus interlocutores.
- Asocie el punto anterior a las estrategias de negocio y la imagen de la empresa en el desarrollo de sus actividades.
- Articule las estrategias de seguridad informática con el proceso de toma de decisiones y los principios de integridad, confidencialidad y disponibilidad de la información.
- Muestre una valoración costo-beneficio, ante una falla de seguridad.
- Desarrolle las justificaciones de la importancia de la seguridad informática en función de hechos y preguntas concretas, que muestren el impacto, limitaciones y beneficios sobre los activos claves de la organización
- Un consejo más, sea oportuno y sagaz para presentar su producto, procurando tener la mayor información del negocio y los riesgos asociados con los activos críticos de la organización.

3.5.3 Las Políticas de Seguridad Informática como base de la administración de la seguridad integral

Las políticas de seguridad informática conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. Conforme a lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos.

Las políticas de seguridad informática constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y continuamente alimentado que observe la concientización, métodos de acceso a la información, monitoreo de cumplimiento y renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

[4]Las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

4 Análisis de Riesgos en la infraestructura de Laboratorio de TI

4.1 Introducción

Este reporte presenta los resultados del análisis de la situación actual del Instituto Mexicano del Petróleo respecto a la seguridad informática.

En él se trata de dar un panorama general de la situación actual del IMP en seguridad informática tomando únicamente como referencia información emanada del Laboratorio de Tecnologías de la Información. Un ejercicio más completo deberá considerar las demás áreas del Instituto.

Para realizar este trabajo se emplearon diversos documentos así como variadas herramientas, las herramientas más importantes empleadas son: Cobra, RUsecure y Nessus. Para las dos primeras herramientas se obtuvieron ejemplares de evaluación y la tercera es software libre. A continuación se describirán dichas herramientas.

4.1.1 COBRA [18]

COBRA. Es una herramienta que examina todas las áreas relacionadas con el estándar ISO17799 desarrollado para gestionar y analizar la seguridad de los sistemas informáticos. Mediante módulos expertos de cuestionarios analiza la situación actual del sistema con respecto a las exigencias del estándar. Su funcionalidad está dirigida, fundamentalmente, a la administración y análisis de los riesgos relacionados con el ámbito de la seguridad en el uso de la tecnología de la información.

Esta herramienta pretende explorar los elementos básicos del riesgo, é introducir una metodología de evaluación de riesgos de seguridad. También abarca el uso de otro producto que ayuda a asegurar el cumplimiento con las políticas de la seguridad, y estándares externos en base al estándar ISO 17799 y la legislación aplicable a cada país.

Consta de dos partes el (Risk Consultant) o Consultor del Riesgo y el (ISO Complianse analyst) o Analista del cumplimiento ISO17799.

COBRA, y su metodología estándar, resulta muy adecuada para abordar estos asuntos correctamente. Fue desarrollado en total cooperación con una de las instituciones financieras principales del mundo y requirió muchos años de investigación.

4.1.1.1 Consultor del Riesgo (Risk Consultant)

Consiste en una gama de herramientas de análisis de riesgos, consultivas y de revisión de la seguridad. Éstas fueron desarrolladas en gran parte siguiendo el

cambio natural de la seguridad de las Tecnologías de la Información, y los requerimientos del negocio sobre estas áreas.

La primer fuente de cambios fue la aceptación cada vez mayor de que la seguridad de TI era un asunto del negocio. Es en gran parte que las revisiones de la seguridad deben estar relacionadas con el negocio, con los costos de soluciones justificadas y las recomendaciones.

Características.

El consultor del riesgo de COBRA provee un servicio completo del análisis del riesgo, compatible con la mayoría de las metodologías reconocidas (cualitativo y cuantitativo). Es un sistema experto basado en cuestionarios y en una base de conocimiento extensa.

Evalúa la importancia relativa de todas las amenazas y vulnerabilidades y genera recomendaciones y soluciones apropiadas. Además, sus informes proporcionan una evaluación escrita y una puntuación o nivel relativo del riesgo, para cada categoría del riesgo. Los riesgos identificados se ligan automáticamente a las implicaciones potenciales (financieras, pérdida del cliente, etc.) para el negocio o el departamento.

Adaptación automática.

No hay dos empresas iguales, mucho menos lo son sus requisitos de seguridad. El consultor del riesgo por lo tanto generará cuestionarios, a partir de los módulos de la base de conocimientos, que satisfagan específicamente a la organización, al ambiente y al sistema bajo evaluación. Esta función también se realiza dinámicamente mientras que se contestan las preguntas y el consultor del riesgo obtiene más información.

Está diseñado para ser verdaderamente analítico. Puede ser utilizado sin la necesidad de conocer detalladamente o de tener experiencia en usar el software de administración de riesgo. No hay necesidad de emplear a consultores costosos para mantener el sistema.

Reportes.

Los reportes producidos por el consultor de riesgo no son salidas de computadoras estándar. Son informes de negocio profesionales y son apropiados para la interpretación de la administración técnica y no técnica.

El Proceso de evaluación del Riesgo.

El proceso de evaluación del riesgo, que usa COBRA, es extremadamente flexible. Un número substancial de métodos son soportados. Sin embargo, el proceso por omisión consiste generalmente en tres etapas:

Construcción del cuestionario.
Encuestas sobre el riesgo.
Generación de reportes.

Durante la primera etapa, vía el módulo de selección o generación, se prepara el cuestionario base para adecuar el ambiente y los requisitos del usuario.

La segunda etapa es el proceso de encuesta - las preguntas del consultor de riesgo son contestadas por el personal apropiado y la información se almacena con seguridad.

Para la tercera etapa la evaluación del riesgo se producen ' puntuaciones ´ para las categorías individuales del riesgo, se hacen las recomendaciones individuales, se ofrecen las soluciones, y se explican las implicaciones potenciales del negocio.

Cada una de estas etapas es manejada por su componente correspondiente en el sistema: Constructor del cuestionario, encuestador del riesgo y generador de reportes.
Cada módulo abarca un área particular del riesgo o de una clase específica de amenaza (Ej. acceso lógico, acceso físico, redes, desarrollo, operaciones, etc.).

Módulos de Preguntas (cuestionarios).

Las preguntas están en varios formatos; respuesta obligatoria, respuesta opcional, respuesta múltiple obligatoria, respuesta múltiple opcional, respuesta de texto, y respuesta numérica. La mayoría son de opción simple y múltiple.

Generador de reportes.

El generador de reportes se utiliza para producir los resultados de los cuestionarios terminados. Los resultados son apropiados para la interpretación de la administración técnica y no técnica y están en forma de un documento profesional de negocio.

Contenido del reporte.

Se proporcionan un conjunto de secciones del reporte:

Soluciones recomendadas y sugerencias adicionales específicas del control de la seguridad.
Una evaluación descriptiva y un porcentaje relativo de riesgo para cada ' categoría de riesgo ' en cada área considerada.
Un análisis completo del impacto para el negocio o el departamento.
Acoplamiento directo entre las áreas de riesgo y las implicaciones financieras del negocio potenciales.

4.1.1.2 Administrador del módulo COBRA (COBRA Module Manager)

El consultor del riesgo de COBRA ***(COBRA Risk Consultant*)** y el administrador del módulo (***Module Manager)*** comparten una biblioteca de las valoraciones del nivel del riesgo. Estas evaluaciones se relacionan con áreas específicas de riesgo o con las categorías individuales de la amenaza. Nuevamente con el administrador del módulo, todo el texto de la evaluación y los datos se pueden cambiar, suprimir o agregar.

También comparten una biblioteca de contra medidas, salvaguardas o de recomendaciones. Nuevamente éstos pueden ser cambiados, agregados o eliminados. Las contra medidas o salvaguardas se pueden también agrupar, para las situaciones donde las múltiples recomendaciones o soluciones son requeridas.

Bases del conocimiento COBRA ***(COBRA Knowledge Bases).***

A 01 evaluación del alto riesgo.
A 02 Evaluación del Riesgo de la Seguridad de TI.
A 03 Evaluación del Riesgo Operacional del Negocio y TI.
D 01 Evaluación del riesgo de la infraestructura de la seguridad electrónica.

Las primeras dos éstos permiten un análisis comprensivo y detallado del riesgo en sus respectivos dominios. La tercera permite una evaluación y una descripción rápida del sistema entero del negocio. La última base de conocimiento fue construida específicamente para cubrir la LAN y los sistemas básicos de red.

4.1.1.3 El Analista del cumplimiento ISO17799 ó (ISO Complianse analyst)

Tiene las mismas funciones que el consultor del riesgo, en lo único que cambian es en las bases del conocimiento que manejan.

Bases del conocimiento para el analista del cumplimiento ISO:

ASSETCLA – Clasificación y control de activos.
BUSCON – Planeación de la continuidad del negocio.
COMNETMA – Administración de las operaciones y equipo de computo.
COMPLIAN – Cumplimiento.
PERSONNE – Seguridad del personal.
PHYSEC – Seguridad física y ambiental.
SECORG – Seguridad de la organización.
SECPOL – Políticas de seguridad.
SYSACC – Sistemas de control de acceso.
SYSDEV – Desarrollo y mantenimiento de sistemas.

4.1.1.4 RUsecure[19]

Políticas de Seguridad de la Información.

Manual y glosario de referencia.

RUSecure. Es una conjunto de productos integrados los cuales ofrecen a la organización las herramientas necesarias para integrar políticas de seguridad de la información, y generar la mejora en sus operaciones de negocio cotidianas.
Las políticas de la seguridad de la información han sido recopiladas de la extensa experiencia de los mejores consultores de la seguridad de la información que han desarrollado proyectos de los sistemas del negocio a través del mundo, y en donde la seguridad de la información ha desempeñado un papel importante. Basado sobre el ISO 17799 y el BS 7799.

Proporciona una extensa gama de políticas, las cuales pueden ser modificadas y adoptadas por su organización y sobre las cuáles puede ser construida una cultura comprensiva de la seguridad de la información.

La versión 2.0 de las políticas de la seguridad de la información incluye estas 3 características importantes adicionales:

1) Notas explicativas que proporcionan mejor entendimiento de la política.

2) Algunos de los tópicos de seguridad de la información importantes que deben ser considerados al implementar la política de seguridad.

3) Las referencias relacionadas al ISO 17799/BS 7799.

4.1.1.5 Nessus[20]

Uno de los pasos que debemos hacer para asegurar una computadora o una red es, analizarla periódicamente, en busca de fallos.

Un analizador (escáner) de seguridad es un software que remotamente, accede a una red dada y determina cuando un agente externo puede entrar en el o dañarlo de algún modo.

El proyecto “Nessus”, trata de proveer a la comunidad de Internet un analizador remoto de seguridad, gratuito, actualizado y fácil de usar.
Este proyecto empezó a principios de 1998, y la primera versión apareció en Abril de 1998. En esta época, el analizador de seguridad más completo era SATAN, que es a la fecha obsoleto, (actualmente ha cuestionado a SARA, que es la herramienta que actualmente se utilizaba en el IMP).

Nadie en especial fundó el proyecto Nessus. Los autores hicieron su parte en su tiempo libre. Los usuarios también usan su tiempo libre para enviar errores y sugerir mejoras.

Nessus es flexible, extensible, y relativamente fácil de usar, busca y detecta un gran número de agujeros de seguridad.

Es una herramienta de seguridad que busca agujeros en nuestro sistema y nos indica los mismo, también nos proporciona cierta información para solucionarlos.

Se trata de una herramienta con una estructura cliente/servidor.

Esta herramienta la podemos utilizar en distintas plataformas:
__ Linux,
__ Solaris,
__ NetBSD,
__ FreeBSD,
__ Microsoft Windows (Client)
__ Java (Client)

Plugins.

Los plugins son el "corazón" de nessus. Estos son las pruebas de seguridad, esto significa descubrir una vulnerabilidad determinada, tiene una gran cantidad de plugins, divididos en grupos. NASL (Nessus Attack Scripting Language) es un leguaje Script parecido al C recomendado para escribir pruebas de seguridad.

4.2 Descripción del Análisis de Riesgos

El análisis fue realizado de la siguiente manera:

4.2.1 Definición del alcance

El primer paso fue definir el alcance del análisis de riesgo.

El alcance es: Todo el Laboratorio de Tecnologías de la Información.

Debido a que el laboratorio de TI no cuenta con un inventario completo de los activos del IMP que se emplean para desarrollar sus funciones, y tampoco cuenta con una clasificación de su información, no se puede describir específicamente los activos evaluados. Sin embargo esto no fue un impedimento para que se realizara un análisis de riesgos muy completó, como se menciona en las notas el primer análisis de riesgos es muy general dado que no tiene una base especifica o anterior de donde se pueda partir.

4.2.2 Realización del Análisis de Riesgos

Se contestaron todos los cuestionarios relacionados a las bases de conocimiento que utiliza COBRA, tanto para el consultor de riesgo como para el analista del cumplimiento ISO17799, primeramente se contestaron los relacionados al analista del cumplimiento ISO17799 y se obtuvo toda la información relacionada a esté.

A continuación se obtuvo el reporte entregado por Cobra, se analizaron los resultados y se ingresaron en una tabla en la cual se relacionan con el ISO17799-1, el BS7799-2 y los controles específicos.

Estos resultados se relacionaron con las políticas publicadas en el documento del RUsecure, obteniendo así las políticas necesarias para el Laboratorio de TI del Instituto Mexicano del Petróleo.

El siguiente paso fue la aplicación de los cuestionarios correspondientes al consultor del riesgo, de igual manera se obtuvo el reporte entregado por Cobra.

De forma adicional se realizó un análisis de vulnerabilidades de red en los host principales o más importantes dentro del Laboratorio de TI.

4.3 Aplicación de los cuestionarios relacionados al ISO17799-1

Estos cuestionarios fueron obtenidos de la herramienta COBRA. Dado que se utilizó una versión de evaluación, fue necesario obtener un archivo temporal, depurarlo y volver a estructurarlo. Dichos cuestionarios están en Ingles por lo que también fue necesario traducirlos, una vez terminado esto se empezó la aplicación de los mismos.

A continuación se describen las áreas o tópicos que fueron contestados:

1. Planeación de la Continuidad del Negocio.
Objetivos:

1. Contrarrestar las interrupciones de las actividades productivas críticas del negocio.
2. Evitar fallas mayores o desastres.

2. Sistemas de Control de Acceso.
Objetivos:

1. Controlar el acceso a la información.
2. Prevenir los accesos no autorizados a sistemas de información.
3. Garantizar la protección de servicios de red.
4. Prevenir los accesos no autorizados a las computadoras.
5. Detectar actividades no autorizadas.
6. Garantizar la seguridad de la información cuando se utilice cómputo móvil o remoto.

3. Desarrollo y Mantenimiento de Sistemas.
Objetivos:

1. Asegurar que la seguridad del sistema esta construida dentro de la aplicación para prevenir pérdidas, abusos, y modificaciones de los datos.
2. Proteger la confidencialidad, autenticidad e integridad de la información.
3. Los proyectos informáticos y sus actividades de soporte deberán de ser conducidos de forma segura.

4. Seguridad Física y Ambiental.
Objetivos:

1. Prevenir el acceso no autorizado a las instalaciones para prevenir pérdida, robo, daño de los bienes y evitar la interrupción de las actividades productivas.
2. Prevenir el robo de información y de los procesos de la empresa.

5. Cumplimiento.
Objetivos:

1. Evitar infringir cualquier norma civil o penal, ley, reglamento, obligación contractual o cualquier requerimiento de seguridad.
2. Asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad.
3. Maximizar la efectividad y minimizar las interferencias hacia y del sistema de auditoria del proceso.

6. Seguridad del Personal.
Objetivo:

1. Reducir el riesgo de error humano, robo, fraude, abuso de la información, sistemas y equipos.
2. Asegurarse que el personal este consiente de las amenazas a la información y sus implicaciones.
3. Apoyar la política corporativa de seguridad en contra de accidentes y fallas y a la vez aprender de estos incidentes.

7. Seguridad de la Organización
Objetivos:

1. Administrar la seguridad de la información dentro de la compañía.
2. Mantener la seguridad de las instalaciones de procesamiento de la información y los activos informáticos accesados por terceros, (proveedores, clientes, etc.).
3. Mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información es ejecutada por terceros (outsourcing).

8. Administración de las Operaciones y equipo de Cómputo
Objetivos:

1. Asegurar la correcta operación de las instalaciones de procesamiento.
2. Minimizar el riesgo de fallas en el sistema.
3. Proteger la integridad del software y la información.

4. Mantener la integridad y disponibilidad del procesamiento de la información y comunicaciones.
5. Asegurar la protección de la información en la red y de la infraestructura que la soporta.
6. Prevenir el daño a los activos y procesos críticos del negocio.
7. Prevenir la pérdida, modificación o mal uso de la información intercambiada entre empresas.

9. Clasificación y Control de Activos
Objetivos:
1. Mantener la protección adecuada de los activos corporativos y garantizar que los activos informáticos reciban un nivel adecuado de protección.

10. Políticas de Seguridad.
Objetivo:
2. Proveer la directriz y el soporte de la Dirección General de la empresa para la seguridad de la información.

Cada tópico mencionado cuenta con un cuestionario independiente, el resultado de los cuestionarios contestados nos da una medida de incumplimiento con cada sección importante de ISO/IEC 17799-1, este resultado es utilizado para detectar y documentar los controles que no existen en este momento y el resultado de éste se utiliza para poder dar una sugerencia clara de lo que es necesario, basado en el BS-7799-2, que es la segunda parte del ISO/IEC 17799-1 y que se refiere a la implementación de los controles necesarios o faltantes para el cumplimiento de esta norma.

También se utilizaron diferentes tipos de tablas (las cuales sé encuentran como anexos), para poder relacionar de una manera más sencilla las siguientes partes:

Controles.

- Controles organizacionales y administrativos.
- Controles físicos y ambientales.
- Controles operacionales.
- Controles técnicos.

Estos controles se relacionan con lo siguiente: amenazas, vulnerabilidades, activos, servicios de seguridad, controles específicos, el ISO/IEC 17799-1 y el BS-7799-2.

4.3.1 Resultados

La siguiente tabla muestra los resultados obtenidos de las encuestas aplicadas en el Laboratorio de TI. La primera columna se refiere al apartado de la Norma ISO 17799 con la recomendación de seguridad, la segunda columna contiene el número de control sugerido por el cuestionario aplicado, la tercera columna

muestra el número de control a aplicar conforme a la BS-2 que es la segunda parte del ISO/IEC 17799-1.

TABLA GENERAL DE RESULTADOS DEL IMP.

Planeación de la continuidad del negocio. (BUSCON).			
ISO17799	**CONTROL**	**BS-2**	**INFORMACIÓN**
11.1.1	3.14	4.9.11	**Proceso de administración de la continuidad del negocio.** Se debe implementar un proceso controlado para el desarrollo y mantenimiento de la continuidad del negocio en toda la organización.
Seguridad del personal. (PERSONNE)			
ISO17799	**CONTROL**	**BS-2**	**INFORMACIÓN.**
6.1.1	3.8.1	4.4.1.1	**Inclusión de la seguridad en las responsabilidades de los puestos de trabajo.** Las funciones y responsabilidades en materia de seguridad, según consta en la política de seguridad de la información de la organización (ver 3.1), deben ser documentadas según corresponda.
6.1.2	3.8.3	4.4.1.2	**Selección y política de personal.** Se deben llevar a cabo controles de verificación del personal permanente en el momento en que se solicita el puesto.
6.1.3	3.8.4	4.4.1.3	**Acuerdos de confidencialidad.** Los empleados deben firmar habitualmente un acuerdo de confidencialidad como parte de sus términos y condiciones iniciales de empleo.
6.2.1	3.9	4.4.2.1	**Formación y capacitación en materia de seguridad de la información.** Todos los empleados de la organización y, cuando sea pertinente, los usuarios externos, deben recibir una adecuada capacitación y actualizaciones periódicas en materia de políticas y procedimientos de la organización.
6.3.1	3.12	4.4.3.1	**Comunicación de incidentes relativos a la seguridad.** Los incidentes relativos a la seguridad deben comunicarse a través de canales gerenciales apropiados tan pronto como sea posible.
6.3.2	3.12	4.4.3.2	**Comunicación de debilidades en materia de seguridad.** Los usuarios de servicios de información deben advertir, registrar y comunicar las debilidades o amenazas supuestas u observadas en materia de seguridad, con relación a los sistemas o servicios.
6.3.3	3.12	4.4.3.3	**Comunicación de anomalías del software.** Se deben establecer procedimientos para la comunicación de anomalías del software.
6.3.4	3.12	4.4.3.4	**Aprendiendo de los incidentes.** Debe haberse implementado mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías.
6.3.5	3.13	4.4.3.5	**Proceso disciplinario.** Debe existir un proceso disciplinario formal para los empleados que violen las políticas y procedimientos de seguridad de la organización.
Cumplimiento.(COMPLIAN)			
ISO17799	**CONTROL**	**BS-2**	**INFORMACIÓN.**
12.1.1	3.10	4.10.1.1	**Identificación de la legislación aplicable.** Se deben definir y documentar claramente todos los requisitos legales, normativos y contractuales pertinentes para cada sistema de información.

12.1.2	3.10	4.10.1.2	**Derecho de propiedad intelectual.** Se deben implementar procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material respecto del cual puedan existir derechos de propiedad intelectual, como derecho de propiedad intelectual, derechos de diseño o marcas registradas.
12.1.3	3.10	4.10.1.3	**Protección de los registros de la organización.** Los registros importantes de la organización deben protegerse contra pérdida, destrucción y falsificación.
12.1.4	3.10	4.10.1.4	**Protección de datos y privacidad de la información personal.** Aplicar controles para proteger la información personal de acuerdo con la legislación pertinente.
12.1.5	3.10	4.10.1.5	**Prevención del uso inadecuado de los recursos de procesamiento de información.** Los recursos de procesamiento de información de una organización se suministran con propósitos de negocio. La gerencia debe autorizar el uso que se da a los mismos.
12.1.6	3.10	4.10.1.6	**Regulación de controles para el uso de criptografía.** Implementar acuerdos, leyes, normas y demás instrumentos para controlar el acceso a los controles criptográficos o el uso de los mismos.
12.1.7	3.10	4.10.1.7	**Recolección de evidencia.** Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos. Cuando la acción implica la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con las normas de evidencia establecidas en la ley pertinente o en las normas específicas del tribunal en el cual se desarrollará el caso.
12.2.1	3.11	4.10.2.1	**Cumplimiento de la política de seguridad.** La gerencia debe garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad. Asimismo, se debe considerar la implementación de una revisión periódica de todas las áreas de la organización para garantizar el cumplimiento de las políticas y estándares de seguridad.
12.2.2	3.11	4.10.2.2	**Verificación de la compatibilidad técnica.** Se debe verificar periódicamente la compatibilidad de los sistemas de información con los estándares de implementación de la seguridad.
12.3.1	3.11	4.10.3.1	**Controles de auditoria de sistemas.** Los requerimientos y actividades de auditoria que involucran verificaciones de los sistemas operacionales deben ser cuidadosamente planificados y acordados a fin de minimizar el riesgo de discontinuidad de los procesos de negocio.
12.3.2	3.11	4.10.3.2	**Protección de las herramientas de auditoría de sistemas.** Se debe proteger el acceso a las herramientas de auditoría de sistemas, por ej. Archivos de datos o software, a fin de evitar el mal uso o el compromiso de las mismas.
Clasificación y control de activos.(ASSETCLA)			
ISO17799	**CONTROL**	**BS-2**	**INFORMACIÓN.**
5.1.1	3.7	4.3.1.1	**Inventario de activos.** Un inventario de todos los activos importantes será redactado y mantenido.
5.2.1	3.7	4.3.2.1	**Pautas de clasificación.** Las clasificaciones y controles de protección asociados de la información, deben tomar cuenta de las necesidades de la empresa con respecto a la distribución o restricción de la información, y de la incidencia de dichas necesidades en las actividades de la organización.
5.2.2	3.7	4.3.2.2	**Etiquetado y manejo de la información.** Es importante que se defina un conjunto de procedimientos adecuados para el etiquetado y manejo de la información, según el esquema de clasificación adoptado por la organización.
Seguridad de la organización.(SECORG)			

ISO17799	CONTROL	BS-2	INFORMACIÓN.
4.1.1	3.2	4.2.1.1	**Foro gerencial sobre seguridad de la información.** Debe tenerse en cuenta la creación de un foro gerencial para garantizar que existe una clara dirección y un apoyo manifiesto de la gerencia a las iniciativas de seguridad.
4.1.2	3.2	4.2.1.2	**Coordinación de la seguridad de la información.** En una gran organización, podría ser necesaria la creación de un foro ínter funcional que comprenda representantes gerenciales de sectores relevantes de la organización para coordinar la implementación de controles de seguridad de la información.
4.1.3	3.2	4.2.1.3	**Asignación de responsabilidades en materia de seguridad de la información.** Deben definirse claramente las responsabilidades para la protección de cada uno de los recursos y por la implementación de procesos específicos de seguridad.
4.1.4	3.2	4.2.1.4	**Proceso de autorización para instalaciones de procesamiento de información.** Debe establecerse un proceso de autorización gerencial para nuevas instalaciones de procesamiento de información.
4.1.5	3.2	4.2.1.5	**Asesoramiento especializado en materia de seguridad de la información.** Asesoramiento especializado en materia de seguridad. Idealmente, éste debe ser provisto por un asesor interno experimentado en seguridad de la información.
4.1.7	3.2	4.2.1.7	**Revisión independiente de la seguridad de la información.** El documento que fija la política de seguridad de la información establece la política y las responsabilidades por la seguridad de la información. Su implementación debe ser revisada independientemente.
4.2.1	3.3	4.2.2.1	**Identificación de riesgos del acceso de terceras partes.** Los riesgos asociados con accesos a las instalaciones de procesamiento de información organizacional por terceras partes deben evaluarse e implementar controles de seguridad apropiados.
4.2.2	3.3	4.2.2.2	**Requerimientos de seguridad en contratos con terceros.** Las disposiciones que contemplan el acceso de terceros a las instalaciones de procesamiento de información de la organización deben estar basadas en un contrato formal que contenga todos los requerimientos de seguridad, o haga referencia a los mismos, a fin de asegurar el cumplimiento de las políticas y estándares (normas) de seguridad de la organización.
Políticas de seguridad.(SECPOL)			
ISO17799	**CONTROL**	**BS-2**	**INFORMACIÓN.**
3.1.1	3.1	4.1.1.1	**Documentación de la política de seguridad de la información.** Los responsables del nivel gerencial deberán aprobar y publicar un documento que contenga la política de seguridad y comunicarlo a todos los empleados, según corresponda.
3.1.2	3.1	4.1.1.2	**Revisión y evaluación.** La política de seguridad debe revisarse regularmente y en caso de cambios influenciados, para asegurar que sigue siendo apropiada.
Sistemas de control de acceso.(SYSACC)			
ISO17799	**CONTROL**	**BS-2**	**INFORMACIÓN.**
9.1.1	6.2	4.7.1.1	**Política de control de accesos.** Se deben definir y documentar los requerimientos de negocio para el control de accesos. Las reglas y derechos del control de accesos, para cada usuario o grupo de usuarios, deben ser claramente establecidos en una declaración de política de accesos.
9.2.1	6.2	4.7.2.1	**Registro de usuarios.** Debe existir un procedimiento formal de alta y baja de usuarios para otorgar acceso a todos los sistemas y

			servicios de información multiusuario.
9.2.2	6.2	4.7.2.2	**Administración de privilegios.** La asignación y uso de privilegios debe restringirse y controlarse.
9.2.3	6.2 y 6.1.1	4.7.2.3	**Administración de contraseñas de usuario**. La asignación de contraseñas debe controlarse a través de un proceso de administración formal.
9.2.4	6.3	4.7.2.4	**Revisión de derechos de acceso de usuario.** La gerencia debe llevar a cabo un proceso formal a intervalos regulares, a fin de revisar los derechos de acceso de los usuarios.
9.3.1	6.1 y 6.1.1	4.7.3.1	**Uso de contraseñas.** Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.
9.4.5	6.5.1	4.7.4.5	**Protección de los puertos de diagnostico remoto.** El acceso a los puertos de diagnostico debe ser controlado de manera segura.
9.4.6	6.5.6	4.7.4.6	**Subdivisión de redes.** Se deben introducir controles dentro de la red, a fin de segregar grupos de servicios de información, usuarios y sistemas de información.
9.4.9	6.5	4.7.4.9	**Seguridad de los servicios de red.** Una clara descripción de los atributos de seguridad de todos los servicio de red usados por la organización debe proveerse claramente.
9.5.2	6.6.2	4.7.5.2	**Procedimientos de conexión de terminales.** El acceso a los servicios de información debe ser a través de un proceso de conexión seguro.
9.5.4	6.1. y 6.1.1	4.7.5.4	**Sistema de administración de contraseñas.** Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.
9.5.7	6.4	4.7.5.7	**Desconexión de terminales por tiempo muerto.** Las terminales inactivas en ubicaciones de alto riego, por ej. Áreas públicas o externas fuera del alcance de la gestión de seguridad de la organización, o que sirven a sistemas de alto riego, deben apagarse después de un periodo definido de inactividad, para evitar el acceso de personas no autorizadas.
9.5.8	6.6.5	4.7.5.8	**Limitación del horario de conexión.** Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo.
9.6.1	6.7.1	4.7.6.1	**Restricción del acceso a la información**. El acceso a la información y a las funciones de los sistemas de aplicación deberán restringirse en conformidad con una política de control de acceso definida.
9.6.2	6.7.2	4.7.6.2	**Aislamiento de sistemas sensibles.** Los sistemas sensibles requieren de un ambiente informático dedicado (aislado).
9.7.1	6.8	4.7.7.1	**Registro de eventos.** Deben generarse registros de auditoria que contengan excepciones y otros eventos relativos a seguridad, y deben mantenerse durante un periodo definido para acceder en futuras investigaciones y en el monitoreo de control de accesos.
9.7.2	6.8	4.7.7.2	**Monitoreo del uso de los sistemas.** Se deberá establecer procedimientos para monitorear el uso de las instalaciones de procesamiento de la información y el resultado de las actividades de monitorización se revisaran regularmente.
9.8.1	3.5	4.7.8.1	**Computación móvil.** Se debe adoptar una política formal que tome en cuenta los riesgos que implica trabajar con herramientas informáticas móviles, en particular en ambientes no protegidos.
9.8.2	3.6	4.7.8.2	**Trabajo remoto.** Se deben desarrollar políticas y procedimientos para autorizar y controlar las actividades del trabajo remoto.
Administración de operaciones y equipo de cómputo.(COMNEMA)			
ISO17799	**CONTROL**	**BS-2**	**INFORMACIÓN.**
8.1.1	5.1	4.6.1.1	**Documentación de los procedimientos operativos.** Se deben documentar y mantener los procedimientos operativos identificados en la política de seguridad en 4.1.1.1.
8.1.2	5.2	4.6.1.2	**Control de cambios en las operaciones.** Se deben controlar los cambios en los sistemas e instalaciones de procesamiento de información.
8.1.3	5.3	4.6.1.3	**Procedimientos de manejo de incidentes.** Se deben establecer responsabilidades y procedimientos de manejo de incidentes para

			garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.
8.1.4	3.8.2	4.6.1.4	**Separación de funciones.** Se debe considerar la separación de la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir las oportunidades de modificación no autorizada o mal uso de la información o los servicios.
8.1.5	5.4	4.6.1.5	**Separación entre instalaciones de desarrollo e instalaciones operativas.** Las instalaciones de desarrollo y prueba deben ser separadas de las instalaciones de operación.
8.1.6	5.5	4.6.1.6	**Administración de instalaciones externas.** Antes de usar un contratista externo para la administración de las instalaciones de procesamiento de información se debe identificar los riesgos con anticipación, y deben acordarse controles adecuados con el contratista e incluirse en el contrato.
8.2.1	5.6	4.6.2.1	**Planificación de la capacidad.** Se deben monitorear las demandas de capacidad y realizar proyecciones de los futuros requerimientos de capacidad, a fin de garantizar la disponibilidad del poder de procesamiento y almacenamiento adecuados.
8.3.1	5.8	4.6.3.1	**Controles contra software malicioso.** Se deben implementar controles de detección y prevención para la protección contra software malicioso, y procedimientos adecuados de concientización de usuarios.
8.4.1	5.9	4.6.4.1	**Resguardo de la información.** Se deben realizar periódicamente copias de resguardo de la información y el software esenciales para la empresa.
8.4.3	5.10	4.6.4.3	**Registro de fallas.** Se deben comunicar las fallas y tomar medidas correctivas.
8.6.1	5.17	4.6.6.1	**Administración de medios informáticos removibles.** Deben implementarse procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos.
8.6.2	5.17	4.6.6.2	**Eliminación de medios informáticos.** Cuando ya no son requeridos, los medios informáticos deben eliminarse de manera segura.
8.6.3	5.17	4.6.6.3	**Procedimientos de manejo de la información.** Se deben establecer procedimientos para el manejo y almacenamiento de la información para protegerla contra su uso inadecuado o divulgación no autorizada.
8.6.4	5.17	4.6.6.4	**Seguridad de la documentación del sistema.** La documentación del sistema debe ser protegida de accesos no autorizados.
8.7.2	5.12	4.6.7.2	**Seguridad de los medios en tránsito.** Los medios que son transportados deben ser protegidos de accesos no autorizados, mal uso o alteración.
8.7.3	5.3	4.6.7.3	**Seguridad del comercio electrónico.** El comercio electrónico debe ser protegido contra actividades fraudulentas, disputas contractuales y divulgación o modificación de información.
8.7.6	5.16	4.6.7.6	**Sistemas de acceso público.** Debe existir un proceso formal de autorización antes de que la información sea pública y disponible y la integridad de tal información debe ser protegida para prevenir modificaciones no autorizadas.
Desarrollo y mantenimiento de sistemas.(SYSDEV)			
ISO17799	**CONTROL**	**BS-2**	**INFORMACIÓN.**
10.1.1		4.8.1.1	**Análisis y especificaciones de requerimientos de la seguridad.** Los requerimientos del negocio para los sistemas nuevos, o las mejoras a los sistemas existentes especificarán los requerimientos para los controles.
10.2.1	7.1	4.8.2.1	**Validación de datos de entrada.** Los datos de entrada en sistemas de aplicación deben ser validados para asegurar que son correctos y apropiados.
10.2.2	7.1	4.8.2.2	**Controles de procesamiento interno.** La revisión validación debe ser incorporada dentro de los sistemas para detectar la corrupción de los datos procesados.
10.2.3	7.1	4.8.2.3	**Autenticación de mensajes.** La autenticación de mensajes debe

			ser usada para las aplicaciones en las cuales exista un requerimiento de seguridad para proteger la integridad del contenido del mensaje.
10.3.1	7.2	4.8.3.1	**Política en el uso de controles criptográficos.** Se desarrollara y seguirá una política en el uso de los controles criptográficos para la protección de la información.
10.4.1		4.8.4.1	**Control del software operativo.** Se debe proveer de control para la implementación de software en los sistemas en operaciones.
10.4.2	5.7	4.8.4.2	**Protección de los datos de prueba del sistema.** Los datos de prueba deben ser protegidos y controlados.
10.4.3		4.8.4.3	**Control de acceso a las bibliotecas de programa fuente.** Se debe mantener un control estricto del acceso a las bibliotecas de programas fuentes.
10.5.1		4.8.5.1	**Procedimientos de control de cambios.** La implementación de los cambios debe ser estrictamente controlada para el uso de procedimientos de control de cambios formales para minimizar la corrupción de los sistemas de información.
10.5.2		4.8.5.2	**Revisión técnica de los cambios en el sistema operativo.** Cuando se realizan cambio, los sistemas de aplicación deben ser revisados y probados.
10.5.4	5.8	4.8.5.4	**Canales ocultos y código troyano.** La compra, uso y modificación de software debe ser controlado y revisado para proteger contra posibles canales ocultos y código troyano.
Seguridad física y ambiental.(PHYSEC)			
ISO17799	**CONTROL**	**BS-2**	**INFORMACIÓN.**
7.1.1	4.1	4.5.1.1	**Perímetro de seguridad física.** Las organizaciones deben utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información.
7.1.2	4.1	4.5.1.2	**Controles de acceso físico.** Controles de acceso físico. Las áreas protegidas deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se permite el acceso de personal autorizado.
7.1.3	4.1	4.5.1.3	**Protección de oficinas, cuartos e instalaciones.** Las áreas protegidas deben ser creadas para proteger oficinas, cuartos e instalaciones con requerimientos de seguridad especiales.
7.1.4	4.1	4.5.1.4	**Desarrollo de tareas en áreas protegidas.** Controles y lineamientos adicionales para el desarrollo de tareas en áreas aseguradas deben ser usados para incrementar la seguridad dada por la protección de los controles físicos del área protegida.
7.1.5	4.1	4.5.1.5	**Aislamiento de las áreas de entrega y carga.** Las áreas de entrega y carga deben ser controladas y, si es posible, estar aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.
7.2.1	4.2	4.5.2.1	**Ubicación y protección del equipo.** El equipo debe ser ubicado o protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.
7.2.5	4.2	4.5.2.5	**Seguridad del equipo fuera del ámbito de la organización.** El uso de equipo destinado al procesamiento de información, fuera del ámbito de la organización, debe ser autorizado por el nivel gerencial.
7.2.6	4.2	4.5.2.6	**Baja segura o re utilización del equipo.** La información debe ser borrada del equipo antes de eliminarlo o re utilizarlo.
7.3.1	4.3	4.5.3.1	**Políticas de escritorios y pantallas limpias.** La organización debe tener e implementar una política de escritorios limpios y pantallas limpias para reducir el riesgo de accesos no autorizados, la pérdida y daño a la información.

Estos resultados sirvieron como entrada para poder generar las políticas necesarias sobre una base sólida y especifica.

4.4 Aplicación de los cuestionarios relacionados al Consultor del Riesgo

La revisión de este módulo de COBRA se estudia para cada cuestionario independientemente, el cuestionario correspondiente a la Evaluación del Riesgo Operacional del Negocio y TI.(A03) no fue contestado por falta de información.

4.4.1 *A 01 evaluación del alto riesgo*

Este cuestionario abarca lo relacionado con la Disponibilidad, Confidencialidad e Integridad.

4.4.1.1 Introducción

El proceso de administración del riesgo operacional a sí mismo se divide en cuatro fases distintas:

1.- Definición del alcance.

El análisis de riesgo se utiliza generalmente para determinar las áreas de riesgo para una unidad de negocio específica. Si el alcance de esta unidad de negocio no se define correctamente y se pueden presentar dificultades é inconsistencias. La primera fase, por lo tanto, es definir correctamente el alcance del ejercicio y acordar que se incluye y que no.

2.- Evaluación del Impacto del Negocio.

Esta fase determina los impactos potenciales al negocio que podrían darse de una amplia gama de amenazas. Los asuntos tales como pérdida de disponibilidad, pérdida de integridad y divulgación de la confidencialidad, son considerados todos en lo referente al valor de la unidad del negocio.

3.- Evaluación del Riesgo.

Esta parte del proceso determina las vulnerabilidades que son inherentes en el sistema o la función del negocio bajo revisión. Los controles existentes, o las contra medidas, también son consideradas permitiendo que cualquier exposición sea identificada.

4.- Administración de Riesgos.

De acuerdo con la información recibida a partir de las fases anteriores, la administración ejecutiva puede entonces decidir si los riesgos deben ser controlados (Ej. Implementación de contra medidas ó salvaguardas recomendadas.), Conservando (Ej.: No hacer nada), o transferida usando un seguro convencional. Este proceso es el aspecto de la administración de riesgos.

Esto es un ejercicio de descripción del ' riesgo en general ', por lo que es probable que cualquier riesgo identificado como inaceptable conduzca a una revisión completa o a un análisis detallado del riesgo del área referida. Esto se puede realizar también manualmente o vía medios automatizados.

4.4.1.2 Alcance de la evaluación

Introducción.

Esta sección del reporte detalla el alcance de la encuesta sobre el impacto del negocio. Incluye una lista de los módulos que se abarcaron y los cuestionarios usados en la prueba. También identifica por quién fueron contestados dichos cuestionarios, así como la fecha en que se terminaron.

Modulo.	Contestado por.	Puesto.	Fecha.
AVAIL	Laboratorio TI	Resp. del área de seguridad	04/12/2003
BIA	Laboratorio TI	Resp. del área de seguridad	04/12/2003
CONFID	Laboratorio TI	Resp. del área de seguridad	04/12/2003
INTEG	Laboratorio TI	Resp. del área de seguridad	04/12/2003

4.4.1.3 Resumen de la administración

Introducción.

Esta sección del informe resume las áreas del riesgo relevantes a la unidad de negocio en revisión. Se producen dos listas de las categorías del riesgo. La primera lista identifica las áreas que se juzga requieren una atención más inmediata, y para las cuáles puede ser requerida un evaluación detallada. La segunda lista identifica las áreas que son menos importantes, pero que pueden requerir una cierta atención. Las dos listas son seguidas por una valoración solo para esas áreas de riesgo que se consideren necesitar atención detallada. También se abarcan las consideraciones relacionadas al negocio. Éstos son los impactos potenciales que podrían resultar de las exposiciones identificadas.

Las categorías siguientes requieren particular atención, una valoración de cada uno aparece en este resumen de administración.

Categorías Sobre Umbral del Riesgo Aceptable.

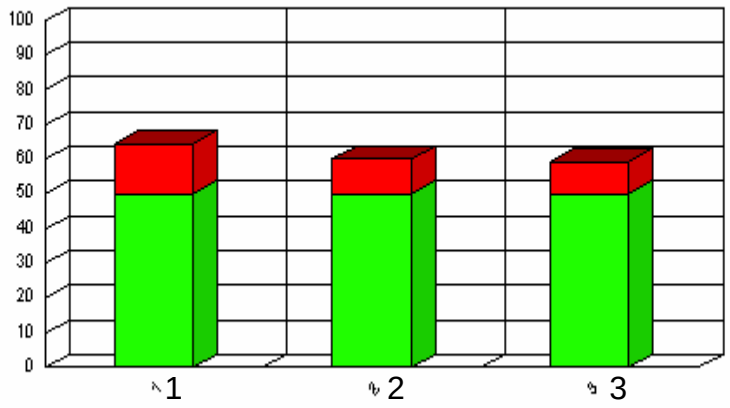

FIGURA 4.1

Categoria de riesgo.	**Factor de riesgo.**
Disponibilidad.	64.33 %
Confidencialidad.	60.27 %
Integridad.	59.19 %

Disponibilidad.

El riesgo de indisponibilidad seria del sistema del negocio, es alto. Se deben tomar las medidas necesarias urgentemente para tratar esto. Se recomienda una revisión específica o una evaluación de riesgos completo para identificar las medidas específicas requeridas.

Confidencialidad.

El riesgo del acceso no autorizado serio a la información, se considera alto. Se deben tomar las medidas inmediatas para rectificar esto. Se recomienda una evaluación de riesgos completa en primera instancia.

Integridad.

El riesgo de la pérdida de integridad de datos, se considera alto. Se debe tomar las acciones necesarias a corto plazo para tratar esto. Se debe emprender urgentemente una revisión completa de la evaluación o de la seguridad del riesgo.

4.4.1.4 Evaluación del Impacto del Negocio

Introducción.

Esta sección proporciona una evaluación detallada de los impactos potenciales del negocio, de las amenazas clásicas, de la pérdida de disponibilidad, de integridad y de confidencialidad. El perfil y valor de la unidad de negocio también es considerado. Los resultados de esta evaluación se pueden utilizar opcionalmente para determinar automáticamente qué asuntos serán examinados posteriormente durante la etapa de la evaluación de riesgos de alto nivel.

El impacto del negocio se presenta en porcentaje, donde cuanto más alto es el porcentaje, mayor es el impacto.

Niveles del Impacto del Negocio.

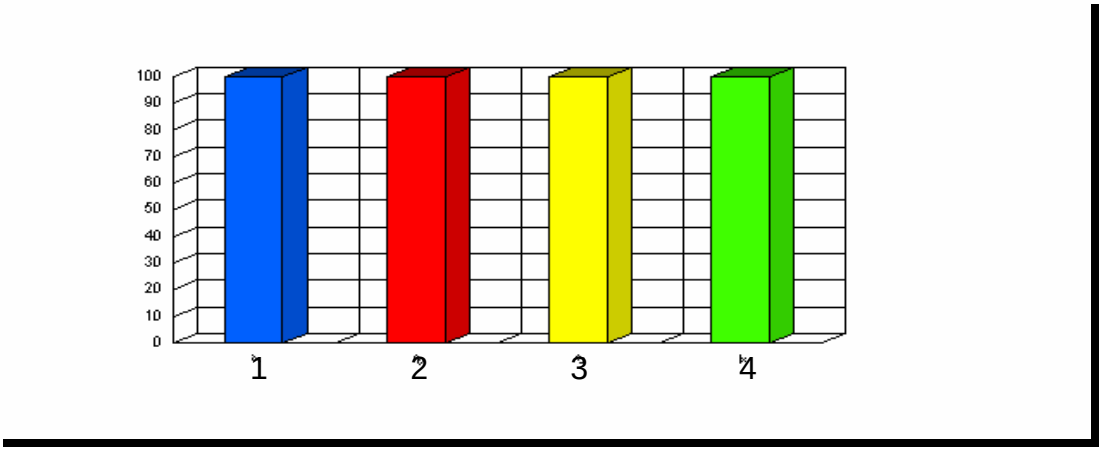

FIGURA 4.2

Categoría del Impacto: 1 - *Impacto del negocio – Disponibilidad.*

Nivel de Impacto: 100 %

Evaluación del Impacto: El impacto de un período relativamente corto de indisponibilidad sería serio. Se aseguraría un efecto significativo sí la recuperación no se recuperara rápidamente.

Categoría del Impacto: 2 -*Impacto del negocio – Confidencialidad.*

Nivel de Impacto: 100 %

Evaluación del Impacto: Un acceso serio a la información/datos confidenciales o importantes podía tener un impacto substancial sobre el negocio.

Categoría del Impacto: 3 -*Impacto del negocio – Integridad.*

Nivel de Impacto: 100 %

Evaluación del Impacto: Una falla seria de integridad en información/datos podía tener un impacto substancial en el negocio.

Categoría del Impacto: 4 - *Perfil del negocio.*

Nivel de Impacto: 100 %

Evaluación del Impacto: El perfil de este negocio función/servicio es significativo.

4.4.1.5 Evaluación del Riesgo detallado

Introducción.

Esta sección del informe produce un ' factor de riesgo ' y una evaluación de la exposición a la pérdida de disponibilidad, integridad y confidencialidad.

El factor de riesgo se presenta como porcentaje, donde cuanto más alto es el porcentaje, mayor es el impacto.

Niveles del Riesgo.

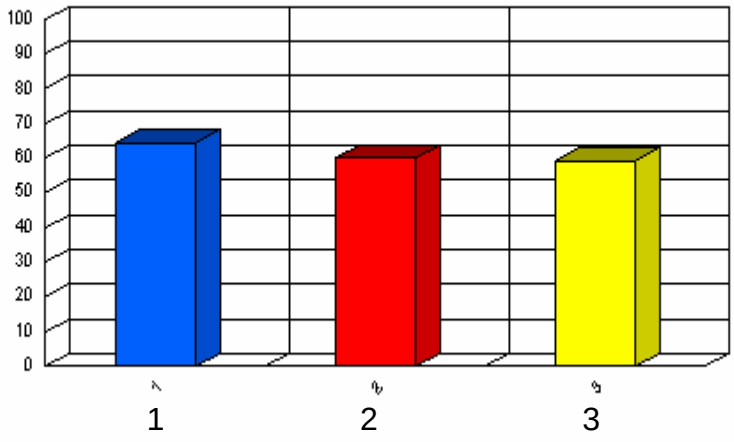

FIGURA 4.3

Categoría del Riesgo:	1- *Disponibilidad.*
Nivel de Riesgo:	64.33 %
Evaluación del Riesgo:	El riesgo de indisponibilidad seria del sistema del negocio es alto. Se deben tomar las medidas urgentes para tratar esto. Se recomienda una revisión específica o una evaluación de riesgos completo para identificar las medidas específicas requeridas.
Categoría del Riesgo:	2 - *Confidencialidad.*
Nivel de Riesgo:	60.27 %
Evaluación del Riesgo:	El riesgo de acceso no autorizado serio a la Información se considera alto. Se deben tomar medidas inmediatas para rectificar esto. Una evaluación de riesgos completo se recomienda en primera instancia.
Categoría del Riesgo:	3 - *Integridad.*
Nivel de Riesgo:	59.19 %
Evaluación del Riesgo:	El riesgo por la pérdida de integridad de los datos se considera alto. Se debe tomar acción a corto plazo para tratar esto. Una revisión completa de la evaluación de la seguridad o del riesgo debe ser realizado urgentemente.

4.4.1.6 Contra medidas o salvaguardas

Introducción.

Esta sección incluye la lista de los asuntos del nivel alto que se deben considerar para reducir o para eliminar las exposiciones identificadas durante la revisión del riesgo.

Disponibilidad.

Se deben tomar las medidas urgentes para reducir la exposición a la indisponibilidad al hardware, equipo y los medios.

Se deben tomar las medidas urgentes para reducir la exposición a la introducción de código malicioso.

Confidencialidad.

Se debe iniciar una revisión detallada para tratar las amenazas de terceros que tienen vistas no autorizadas de la salida de información confidencial o sensible de una impresora.

Los controles o las prácticas de acceso físicos al edificio no son adecuadas. Se deben tomar las medidas inmediatas para tratar esta situación.
Los controles o las prácticas de acceso físicos para las áreas que pueden mantener información sensible/confidencial deben ser aumentados. Las medidas se deben tomar con urgencia.

Los controles de acceso lógicos no son suficientes para proteger datos/información sensible contra escritura externa no autorizada. Se requiere la acción correctora inmediata.

Integridad.

Una amenaza significativa de falla intencional seria durante el ingreso de datos/información importante puede existir. Debe ser emprendida una revisión adicional de esta materia.

Los controles para prevenir la modificación no autorizada del código fuente de programas no parecen apropiados. Debe ser conducida una revisión completa de esta materia.

Los controles de acceso lógicos pueden no ser suficientes para proteger datos/información sensible contra accesos externos no autorizados. Una revisión de este asunto debe ser realizada.

Los controles de acceso lógicos pueden no ser apropiados y suficientes para proteger datos/información sensible contra accesos internos no autorizados. Se debe emprender una revisión adicional de esta materia.

Nota: Estos resultados son parciales ya que cobra entrega los reportes en Ingles, únicamente se tradujo parte del reporte.

4.4.2 *A 02 Evaluación del Riesgo de la Seguridad de TI*

Este cuestionario abarca lo correspondiente al Riesgo de la seguridad de Tecnologías de la Información.

4.4.2.1 Introducción

El análisis operacional de riesgo es un componente esencial a poner sobre una base objetiva, y así permitir que el riesgo sea manejado con eficacia.

Los impactos identificados se utilizan para determinar qué áreas y asuntos deben ser considerados a futuro. Esta unión es extremadamente importante, pues se utiliza para justificar recomendaciones y conclusiones.

El proceso de administración del riesgo operacional a su vez se divide en cuatro fases distintas:

1.- Definición del alcance.

2.- Evaluación del Impacto del Negocio.

3.- Evaluación del Riesgo.

4.- Administración de Riesgos.

Ya definidos anteriormente.

De acuerdo con la información recibida a partir de las fases anteriores, la administración ejecutiva puede entonces decidir si los riesgos deben ser controlados (Ej. Implementación de contra medidas ó salvaguardas recomendadas.), Conservando (Ej. No hacer nada), o transferida usando un seguro convencional. Este proceso es parte de la administración de riesgos.

El número del personal implicado en el proceso varía, dependiendo del alcance y de los impactos potenciales del negocio. Mientras que el alcance sea mayor y los impactos lleguen a ser mayores, más áreas del riesgo serán determinadas. Este personal podría ser de diferentes partes de la unidad de negocio, incluyendo la administración ejecutiva, usuarios y personal de TI.

El producto final del proceso completo es este informe. Contiene toda la información que es necesaria para que la gerencia ejecutiva determine qué acción, si la hay, se debe tomar por lo que se refiere al riesgo operacional.

4.4.2.2 Alcance de la evaluación

Introducción.

Esta sección detalla el alcance de la encuesta sobre el impacto del negocio. Incluye una lista de los módulos que se abarcaron y los cuestionarios usado en la prueba. También identifica por quién fueron contestados dichos cuestionarios, así como la fecha en que se terminaron.

Modulo.	Contestado por.	Puesto.	Fecha.
BUSINESS	Laboratorio TI	Res. del área de seguridad	15/02/2004
SECMGMNT	Laboratorio TI	Res. del área de seguridad	15/02/2004
SYS-ACC	Laboratorio TI	Res. del área de seguridad	15/02/2004
SYS-OTHR	Laboratorio TI	Res. del área de seguridad	15/02/2004
SYSTEM	Laboratorio TI	Res. del área de seguridad	15/02/2004

4.4.2.3 Resumen de administración

Introducción.

Esta sección resume las áreas del riesgo relevantes a la unidad de negocio en revisión. Se producen dos listas de las categorías del riesgo. La primera lista identifica las áreas que se juzgan por requerir una atención más inmediata, y para las cuáles puede ser requerida una evaluación detallada. La segunda lista identifica las áreas que son menos importantes, pero que pueden requerir una cierta atención. Las dos listas son seguidas por una valoración sólo para las áreas del riesgo que se consideran necesitan atención detallada. Las consideraciones relacionadas al negocio también se abarcan. Éstos son los impactos potenciales que podrían resultar de las exposiciones identificadas.

Las categorías siguientes requieren particular atención, una valoración de cada una aparece en este resumen de administración.
Éstos son los impactos potenciales que podrían resultar de las exposiciones identificadas.

Las categorías siguientes requieren la atención particular, una evaluación de cada uno aparece en este resumen de administración.

Categorías Sobre el Umbral del Riesgo Aceptable.

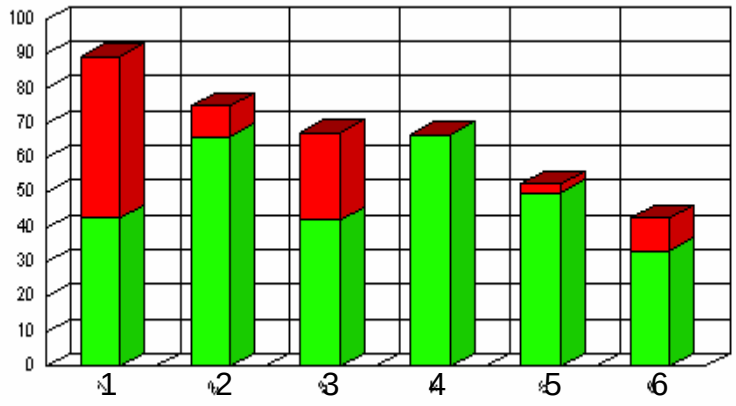

FIGURA 4.4

Categoria de riesgo.	**Factor de riesgo.**
1 - Conocimiento General de la Seguridad	89.29 %
2 - Prácticas de administración de la Seguridad	75.00 %
3 - Política de Seguridad – Contenido	67.31 %
4 - Operación de Sistemas y Componentes de Auditoria	66.67 %
5 - Política de Seguridad – Alcance.	52.63 %
6 - Operación de Sistemas y Componentes del Sistema	42.86 %

Consideraciones Relacionadas al Negocio:

Los datos son relativamente sensibles y confidenciales. El acceso podía tener un impacto financiero mensurable con pérdida del cliente, y juicio legal.

La pérdida potencial máxima debido a la actividad fraudulenta es significativa (estimado en el rango de $10.000 a $100.000).

La pérdida financiera máxima debido a la modificación no autorizada de datos y su pérdida consecuente de integridad es relativamente limitadas. Se considera estar entre $1.000 y $10.000.

Categoría del Riesgo: *Conocimiento General de la Seguridad.*

El nivel del conocimiento de la seguridad es bajo, con un correspondiente aumento en el riesgo de problemas de seguridad. Esto se debe tratar rápidamente con nuevas iniciativas y medidas adicionales.

Categoría del Riesgo: *Prácticas de la administración de la Seguridad.*

Las prácticas de administración de la seguridad esta por debajo del estándar y no mantiene controles de seguridad.

Categoría del Riesgo: *Política de Seguridad – Contenido.*

La política es pobre en varias áreas importantes. Las omisiones pueden aumentar algunos riesgos. La política debe ser realzada más a fondo.

Categoría del Riesgo: *Operación de Sistemas y Componentes de auditoria.*

La auditoria del nivel de sistema es débil en número de relatividad y no soporta completamente otros controles. La mejora y el realce ayudaran de cierta manera a mejorar la seguridad y a reducir los riesgos.

Categoría del Riesgo: *Política de Seguridad – Alcance.*

La política de seguridad no es completamente comprensiva y completa. Algunos aspectos de la seguridad no se abarcan. Esto puede potencialmente tener un efecto perjudicial en los niveles de seguridad en ciertas áreas, aumentando el riesgo.

Categoría del Riesgo: *Operación de Sistemas y Componentes del Sistema.*

El riesgo de dificultad seria através de la exposición de la operación de sistemas o los componentes del sistema es moderado. Los controles están desarrollados pero pueden requerir cierta atención.

4.4.2.4 Evaluación del Impacto del Negocio

Introducción.

Esta sección proporciona una evaluación detallada de los impactos potenciales del negocio de una amplia gama de amenazas. Los resultados de esta evaluación se pueden utilizar opcionalmente para determinarse automáticamente qué áreas serán examinadas posteriormente en un análisis de riesgos detallado.

El análisis del impacto del negocio cubre generalmente el impacto resultado de la indisponibilidad, pérdida de integridad de datos, y pérdida de confidencialidad, así como la determinación del valor de los activos de la unidad de negocio.
El impacto del negocio se presenta como porcentaje, donde cuanto más alto es el porcentaje, mayor es el impacto.

Niveles del Impacto del Negocio.

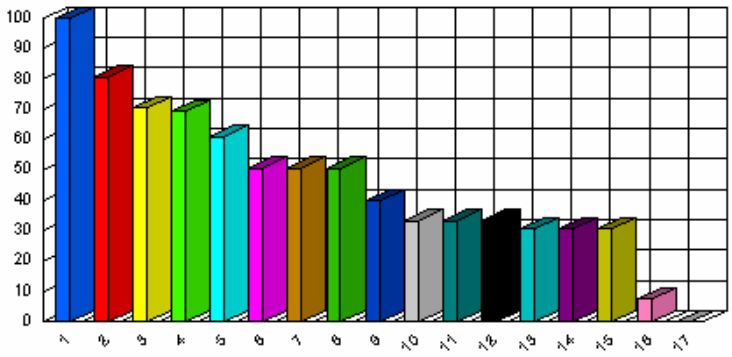

FIGURA 4.5

Categoría del Impacto: 1 - *Pérdida debido a la Indisponibilidad del Sistema.*

Nivel de Impacto: 100 %

Evaluación del Impacto: Si el sistema estuviera indisponible por un período prolongado, la pérdida potencial sería substancial, y podría ser crítica. Estimado en más de $1 millón.

Categoría del Impacto: 2 - *Indisponibilidad - Tiempo Critico.*

Nivel de Impacto: 80.63 %

Evaluación del Impacto: La indisponibilidad del sistema, por un período corto, podía causar pérdida financiera severa. La pérdida financiera potencial es estimada en más de $ 1 millón.

Categoría del Impacto: 3 - *Pérdida Financiera por error de Funcionamiento.*

Nivel de Impacto: 70.53 %

Evaluación del Impacto: Los problemas o el error de funcionamiento podían causar pérdida financiera considerable. La pérdida potencial máxima estimada está en el rango de $100.000 a $1 millón.

Categoría del Impacto: 4 - *Reemplazo y reconstrucción del Equipo.*

Nivel de Impacto: 69.47 %

Evaluación del Impacto: Los costos de reconstrucción, restauración y reemplazo de equipo son extremadamente altos. Estimado en el rango de $100.000 a $1 millón.

Categoría del Impacto: 5 - *Costo del reemplazo de Datos, Software, etc.*

Nivel de Impacto: 60.95 %

Evaluación del Impacto: El costo de reconstruir archivos de datos y de remplazar software, documentación, etc. es significativo.

Categoría del Impacto: 6 - *Sensibilidad y confidencialidad de los Datos.*

Nivel de Impacto: 50.53 %

Evaluación del Impacto: Los datos son relativamente sensibles y confidenciales. El acceso podía tener un impacto financiero importante con pérdida del cliente, juicio, etc.

Categoría del Impacto: 7 - *Fraude Potencial.*

Nivel de Impacto: 50.53 %

Evaluación del Impacto: La pérdida potencial máxima debido a la actividad fraudulenta es significativa. (estimado en el rango de $10.000 a $100.000).

Categoría del Impacto: 8 – *Costo de Reemplazo y capacitación del Personal.*

Nivel de Impacto: 50.53 %

Evaluación del Impacto: El costo de capacitación en el sistema-específico es considerable (estimado para estar en el rango de $10.000 a $100.000).

Categoría del Impacto: 9 - *Reemplazo del Equipo.*

Nivel de Impacto: 40.00 %

Evaluación del Impacto: Los costos de reemplazo del equipo son importantes. Estimado para estar en el rango de $10.000 a $100.000.

Categoría del Impacto: 10 - *Indisponibilidad: acción civil legal.*

Nivel de Impacto: 33.33 %

Evaluación del Impacto: La indisponibilidad del sistema podía conducir a un juicio civil legal.

Categoría del Impacto: 11 - *Indisponibilidad - Confianza del Mercado.*

Nivel de Impacto: 33.33 %

Evaluación del Impacto:	La pérdida de confianza del mercado podía llegar a ser perjudicial a la empresa después de la indisponibilidad del sistema por una semana.
Categoría del Impacto:	12 - *Indisponibilidad: Visibilidad/Reputación.*
Nivel de Impacto:	33.33 %
Evaluación del Impacto:	El servicio proporcionado por este sistema es relativamente visible externamente. Podía resultar de la indisponibilidad un cierto cambio en la reputación y potencialmente a una reducción de la confianza en la empresa.
Categoría del Impacto:	13 - *Pérdida del cliente por Indisponibilidad.*
Nivel de Impacto:	30.33 %
Evaluación del Impacto:	La pérdida del cliente podía alcanzar un nivel crítico después de una semana de indisponibilidad del sistema.
Categoría del Impacto:	14 - *Modificación no autorizada de Datos.*
Nivel de Impacto:	30.53 %
Evaluación del Impacto:	La pérdida financiera máxima debido a la modificación no autorizada de datos y su pérdida consecuente de integridad es relativamente limitadas. Se considera estar entre $1.000 y $10.000.
Categoría del Impacto:	15 - *Pérdida financiera por error de Software.*
Nivel de Impacto:	30.53 %
Evaluación del Impacto:	El error del software podía dar lugar a pérdida financiera mensurable pero no crítica. La pérdida potencial máxima estimada está entre $1.000 y $10.000.
Categoría del Impacto:	16 - *Sistemas Dependientes.*
Nivel de Impacto:	7.42 %

Evaluación del Impacto: No hay sistemas dependientes sobre éste, o la pérdida máxima por los sistemas dependientes por indisponibilidad es mínima.

Categoría del Impacto: 17 – *Implicaciones Reguladoras por Indisponibilidad.*

Nivel de Impacto: 30.53 %

Evaluación del Impacto: No hay implicaciones legislativas o reguladoras por indisponibilidad por un período prolongado.

4.4.2.5 Evaluación del Riesgo Detallado

Introducción.

Esta sección del informe produce un ' factor de riesgo ' y una evaluación detallada para cada área del riesgo incluida en la evaluación del riesgo.
El factor de riesgo se presenta como porcentaje, donde cuanto más alto es el porcentaje, mayor es el impacto.

Niveles del Riesgo.

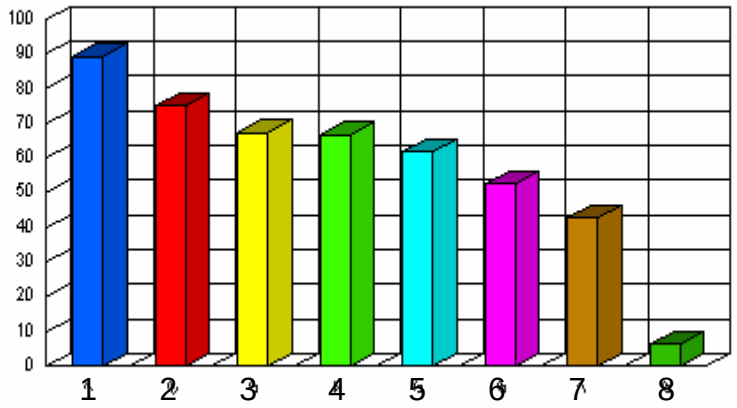

FIGURA 4.6

Para este informe los resultados que se tienen que analizar en esta parte del reporte se pueden revisar en la parte de resumen de la administración, visto anteriormente en el punto 4.4.2.3.

4.4.2.5 Contra medidas

Introducción.

Esta sección incluye la lista de las contra medidas o salvaguardas que se deben considerar para reducir o para eliminar las exposiciones identificadas durante la evaluación de riesgos.

Mientras que el resumen de administración detalla las áreas del sistema que se consideran estar en riesgo, este informe explica qué se debe hacer para eliminar o para reducir el riesgo.

Categoría del Riesgo: *Conocimiento General de la Seguridad.*

Todo el personal nuevo debe ser informado de las políticas y estándares de seguridad y de sus propias responsabilidades con respecto a esto.
Los empleados deben ser instruidos para enfrentar a visitantes desconocidos, y llevarlos a recepción o al lugar donde deben estar.

Los usuarios deben ser informados que serían responsables por las pérdidas resultando del acceso de contraseñas confidenciales.

Se debe iniciar un programa para mejorar el conocimiento de la seguridad. Esto puede incluir seminarios/cursos, boletines de noticias de la seguridad, etc.

Categoría del Riesgo: *Prácticas de la administración de la Seguridad.*

Las responsabilidades de ingreso de datos operacionales, o de desarrollo y deben ser delineadas y realizadas claramente por diversos empleados.

La política de la seguridad es de poco valor si no se hace cumplir realmente. La aplicación forzosa de la política debe ser primordial y todos los mecanismos de seguridad deben estar activados.

A todos los recursos se les debe asignar un dueño específico, incluso si éste no es realmente el responsable actual. El dueño debe estar requerido para especificar un nivel de protección.

La responsabilidad de coordinación de la seguridad debe ser asignada específicamente.

Categoría del Riesgo: *Política de Seguridad – Contenido.*

Todos los sistemas deben estar completamente y adecuadamente asegurados. Se debe incluir la disposición por la perdida física del equipo y la pérdida consecuente debido a la indisponibilidad funcional.

Para las instalaciones sensibles, la publicidad y los viajes innecesarios deben ser evitados.

Un índice de toda la información sensible impresa debe ser mantenido. Debe incluir información tal como: el nivel de seguridad de cada documento, su destino, etc.

Todos los recursos de los datos deben tener un nivel o una etiqueta de seguridad. Esto se podría utilizar para restringir el acceso y/o para identificar sensibilidad relativa.

Categoría del Riesgo: *Operación de Sistemas y Componentes de auditoria.*

La salida de código de todos los sistemas críticos seguros/sensibles se debe revisar/examinar sobre una base regular.

Los expedientes de actividad del sistema se deben analizar para identificar las violaciones de la seguridad y los intentos de violación sobre una base regular (preferiblemente diariamente).

La colección de expedientes de la actividad del sistema debe ser considerada cuidadosamente desde un punto de vista seguro.

Categoría del Riesgo: *Política de Seguridad relacionada al Personal.*

Una cláusula detallando las responsabilidades de seguridad debe ser incluida en todos los contratos de todos los vendedores/surtidores que tengan acceso a los datos, a los recursos o a las premisas de la organización.

Una cláusula detallando las responsabilidades de seguridad debe ser incluida en los contratos de todos los ingenieros y personal de mantenimiento.

La política de la seguridad debe prohibir específicamente el almacenamiento de contraseñas de, terminales con funciones importantes en discos con programas de conexión automática.

Donde es posible se debe usar software para restringir el uso no autorizado de los recursos.

Categoría del Riesgo: *Política de Seguridad – Alcance.*

Las auditorias detalladas y comprensivas de la seguridad se deben realizar por lo menos sobre una base periódica por especialistas externos, consultores o un departamento interno especialista. Los informes deben ser copiados para los usuarios y administradores de sistemas, así como a la administración de la organización.

La política de seguridad y el programa del conocimiento deben abarcar al usuario y al personal de TI.

La política de seguridad debe abarcar software de aplicación.

La política de la seguridad debe abarcar todos los aspectos de ingreso, proceso y salida de datos. La protección y el control de datos deben formar una pieza base de la política.

Categoría del Riesgo: *Operación de Sistemas y Componentes del Sistema.*

El acceso y los cambios a las bibliotecas deben ser controlados por el software de seguridad y un procedimiento rígido de control de cambios.

Cuando los datos o el software se recibe de una organización externa, se debe verificar la integridad para asegurarse de que fue enviada realmente de la organización fuente (ej. Una llamada telefónica). Si los resultados son negativos, los datos/software deben ser aislados y no ser instalados.

Todas los parches a los componentes del sistema operativo, incluyendo parches de emergencia, se deben comprobar/verificar antes de usarse.

Categoría del Riesgo: *Sistemas de acceso y soporte de Sistemas.*

Las contraseñas se debe elegir por los usuarios que dan soporte al sistema quienes tiene asignado un identificador de usuario, a menos que las características del sistema hagan esto imposible.

Las contraseñas deben tener el tiempo de vida práctico más corto. Deben tener asignadas una vida limitada y al final de este tiempo deben ser cambiadas.

Los terminales deben ser deshabilitadas o la identificación del usuario revocada después de un número predefinido de intentos de conexión fallidos. Tres es el número recomendado.

4.4.2.6 Principios Obligatorios

Introducción.

Esta sección identifica los principios y estándares de seguridad generales que son apropiados para la función bajo revisión. Se publican como lista de comprobación de conformidad para el negocio, para asegurarse de que la política y los procedimientos recomendados se están siguiendo.

Se debe proporcionar la documentación formal que describa el acercamiento del sistema de seguridad. Debe incluir los detalles de los mecanismos de la seguridad y cómo se ligan a la política de seguridad del sistema.

La documentación debe también abarcar el uso de las funciones de la seguridad para todos los acontecimientos relacionados a la seguridad, incluyendo: comienzo y cierre del sistema, accesos al recurso, asignación de los atributos de seguridad y validación/verificación.

Debe incluir la implementación de las características y los controles de seguridad y una explicación completa de ellas.

Debe existir un sistema para permitir que los cambios a las siguientes partes puedan ser controlados con seguridad: código ejecutable, código fuente, documentación (desarrollo, diseño y operacional).

El sistema debe proporcionar un mecanismo de control comprensivo de la seguridad.
Nota: Estos resultados son parciales ya que cobra entrega los reportes en Inglés, únicamente se tradujo parte del reporte.

4.4.3 *D 01 Evaluación del riesgo de la infraestructura de la seguridad electrónica*

Este cuestionario abarca lo correspondiente al Riesgo de la Infraestructura de Seguridad Electrónica.

Introducción.

La seguridad en cualquier sistema debe ser proporcional con sus riesgos. Sin embargo, el proceso para determinar qué controles de seguridad son apropiados y rentables es a menudo una cuestión compleja y subjetiva. Una de las principales funciones del análisis de riesgos operacional es poner este proceso sobre una base más objetiva.

Este informe fue producido seguido de la aplicación de una metodología de análisis de riesgos probada.

Objetivos del reporte.

Este reporte es utilizado para cubrir todos los riesgos operacionales pertinentes al sistema/red bajo revisión. La evaluación identificó todas las vulnerabilidades relevantes, y estableció si se encontraban los controles suficientes para contra restarlas. Un factor de riesgo se produce para cada área, y cuando es apropiado se detallan las soluciones recomendadas.

Además son considerados, los impactos potenciales que podrían resultar de una falla de seguridad. Estos impactos cubren la pérdida de integridad de datos, el acceso a los datos, y la indisponibilidad. Se incluye el resumen de administración, los impactos potenciales del negocio se ligan a las exposiciones identificadas. Esto permite a la administración dirigir gasto de la manera más rentable.

Uso del reporte.

Una gama diversa de secciones está disponible. Sin embargo, se da una primera dirección común y rápida.

El resumen de la administración se puede revisar primero para comprobar las áreas que tienen mayor necesidad de atención, y para establecer las implicaciones potenciales de estas exposiciones. Más detalles de las exposiciones se puede obtener entonces de la evaluación de riesgo. Finalmente, las medidas que se pueden tomar para manejar la situación, y para reducir cada una de las exposiciones, también se dan el reporte de las contra medidas o salvaguardas.

4.4.3.1 Alcance de la evaluación

Introducción.

Esta sección del reporte detalla el alcance de la encuesta. Incluye una lista de los módulos que se abarcaron y los cuestionarios usados en la prueba. También identifica por quién fueron contestados dichos cuestionarios, así como la fecha en que se terminaron.

Modulo.	Contestado por.	Puesto.	Fecha.
ACCESS	Laboratorio de TI	Res. Área de seguridad	15/02/2004
AUDIT	Laboratorio de TI	Res. Área de seguridad	15/02/2004
BACKUP	Laboratorio de TI	Res. Área de seguridad	15/02/2004
CHGCTL	Laboratorio de TI	Res. Área de seguridad	15/02/2004
COMSMSGR	Laboratorio de TI	Res. Área de seguridad	15/02/2004
DIAL-IN	Laboratorio de TI	Res. Área de seguridad	15/02/2004
FIREWALL	Laboratorio de TI	Res. Área de seguridad	15/02/2004
IMPACT	Laboratorio de TI	Res. Área de seguridad	15/02/2004
INTERNET	Laboratorio de TI	Res. Área de seguridad	15/02/2004
NETWORK	Laboratorio de TI	Res. Área de seguridad	15/02/2004
PHYSICAL	Laboratorio de TI	Res. Área de seguridad	15/02/2004
POLICY	Laboratorio de TI	Res. Área de seguridad	15/02/2004
SECPKG	Laboratorio de TI	Res. Área de seguridad	15/02/2004
VIRUS	Laboratorio de TI	Res. Área de seguridad	15/02/2004

4.4.3.2 Evaluación del Riesgo Detallado.

Introducción.

Esta sección del informe produce un ' factor de riesgo ' y una evaluación detallada para cada área del riesgo incluida en la evaluación del riesgo. El factor de riesgo se presenta como porcentaje, donde cuanto más alto es el porcentaje, mayor es el impacto.

Niveles del Riesgo.

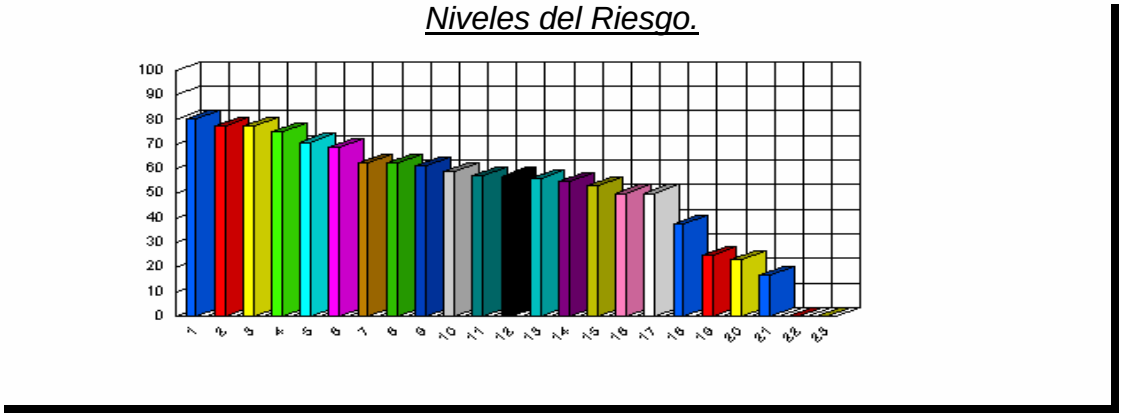

FIGURA 4.7

Categoría del Riesgo: 1 - *Política y administración de la Seguridad.*

Nivel de Riesgo: 88.18 %

Evaluación del Riesgo: La política de seguridad es incomprensible, no esta completa y las practicas de administración de la seguridad está en carencia. Es probable que esto tenga un efecto perjudicial en el nivel de seguridad en un número de áreas, aumentando el riesgo. Es esencial tomar acción sobre esto.

Categoría del Riesgo: 2 - *Acceso a las instalaciones y datos del Sistema.*

Nivel de Riesgo: 77.50 %

Evaluación del Riesgo: Los mecanismos de seguridad en el sistema son relativamente débiles. El acceso a las instalaciones y a los datos del sistema se controlan inadecuadamente. Se requiere una revisión.

Categoría del Riesgo: 3 - *Seguridad física de activos individuales.*

Nivel de Riesgo: 77.50 %

Evaluación del Riesgo: La protección física de acceso a los activos individuales (medios, informes, etc.) es pobre. Los procedimientos y las prácticas no reflejan las amenazas planteadas. Se requieren controles más fuertes.

Categoría del Riesgo: 4 - *Contingencia de la red de área local.*

Nivel de Riesgo: 75.00 %

Evaluación del Riesgo: O no existen acuerdos de contingencia para la red de área local ó los arreglos son débiles e ineficaces. Se debe dar atención con urgencia a esta área.

Categoría del Riesgo: 5 - *Instalaciones Criptográficas en la LAN.*

Nivel de Riesgo: 70.83 %

Evaluación del Riesgo: Las instalaciones criptográficas para los datos que pasan por la red de área local son débiles y necesitan revisión. Esto es particularmente importante donde los datos son confidenciales y donde es esencial su integridad.

Categoría del Riesgo: 6 – *Control de Cambios.*

Nivel de Riesgo: 68.75 %

Evaluación del Riesgo: Los procedimientos del control de cambios son incompletos y subdesarrollados. El sistema tiene un número importante de vulnerabilidades en esta área. Los se deben desarrollar procedimientos más a fondo y hacer que se cumplan estrictamente.

Categoría del Riesgo: 7 – *Procedimiento y administración de auditoria.*

Nivel de Riesgo: 62.50 %

Evaluación del Riesgo: Los procedimientos y la administración de

auditorias están en un estándar relativamente pobre, esto incrementa el riesgo de una violación desapercibida a la seguridad. Esto se debe revisar en la primera oportunidad que se tenga para asegurarse de que un se mantiene un registro comprensivo de la actividad.

Categoría del Riesgo: 8 – *Controles y prácticas del cortafuegos.*

Nivel de Riesgo: 62.50 %

Evaluación del Riesgo: Algunos controles y prácticas desarrolladas del cortafuegos están definidas e implementadas inadecuadamente. fueron identificadas exposiciones potenciales las cuales requieren alguna atención.

Categoría del Riesgo: 9 – *Acceso y uso de Internet.*

Nivel de Riesgo: 61.11 %

Evaluación del Riesgo: Existen defectos claros con respecto a las prácticas de uso y acceso a Internet. Se requiere solucionar este problema.

Categoría del Riesgo: 10 – *Prácticas de respaldos del Sistema y de Datos.*

Nivel de Riesgo: 59.09 %

Evaluación del Riesgo: Las prácticas de respaldo para las Pc's son débiles. Esta área debe ser revisada tan pronto como sea posible.

Categoría del Riesgo: 11 – *Acceso a los datos sensibles.*

Nivel de Riesgo: 57.14 %

Evaluación del Riesgo: La protección de datos sensibles puede no ser suficiente. Un número de exposiciones son evidentes.

Categoría del Riesgo: 12 – *Control de acceso y autenticación.*

Nivel de Riesgo: 56.90 %

Evaluación del Riesgo: Los mecanismos de control de accesos y autentificación son básicos, produciendo una protección incompleta. Un acercamiento más comprensivo debe ser considerado.

Categoría del Riesgo: 13 – *Acceso Lógico a (Ruteadores).*

Nivel de Riesgo: 56.00 %

Evaluación del Riesgo: El acceso lógico a los ruteadores es controlado razonablemente bien. Sin embargo, algunas exposiciones potenciales fueron identificadas y deben ser investigadas.

Categoría del Riesgo: 14 – *Mantenimiento de la red de área local.*

Nivel de Riesgo: 55.00 %

Evaluación del Riesgo: Los procedimientos de mantenimiento del hardware para la red de área local tienen un número de debilidades, creando exposición. Los controles y procedimientos se deben mejorar en un corto plazo.

Categoría del Riesgo: 15 – *Instalaciones Dial-in en la red de área local.*

Nivel de Riesgo: 53.06 %

Evaluación del Riesgo: La administración y el control de las Instalaciones dial-in son débiles, exponiendo el sistema al riesgo. Se deben aplicar las recomendaciones rigurosamente.

Categoría del Riesgo: 16 – *Soporte y Mantenimiento de ruteadores.*

Nivel de Riesgo: 50.00 %

Evaluación del Riesgo: Las prácticas de soporte y mantenimiento para los ruteadores de la red son razonablemente fuertes. Sin embargo, se identificaron algunas debilidades que pueden necesitar atención a corto plazo.

Categoría del Riesgo: 17 – *Detección y administración del Virus.*

Nivel de Riesgo: 50.00 %

Evaluación del Riesgo: Las prácticas de administración de virus tienen varias áreas débiles, que aumentan el riesgo de un ataque que tendría cierto impacto. Éstos se deben revisar y tomar la acción correctora en cuanto se tenga oportunidad.

Categoría del Riesgo: 18 – *Administración de la red de área local.*

Nivel de Riesgo: 37.50 %

Evaluación del Riesgo: Los procedimientos de administración de la red de área local son razonablemente fuertes, aunque algunas áreas pueden requerir revisión.

Categoría del Riesgo: 19 – *Respaldos y Contingencias.*

Nivel de Riesgo: 25.00 %

Evaluación del Riesgo: Los acuerdos de contingencia son generalmente buenos. Puede tener un o dos defectos, que deben ser tratados.

Categoría del Riesgo: 20 – *Mantenimiento del Hardware.*

Nivel de Riesgo: 23.13 %

Evaluación del Riesgo: El cuidado y el mantenimiento del hardware está dentro de un estándar razonable. Aunque algunos problemas son probables en esta área, se deben aplicar las medidas recomendadas.

Categoría del Riesgo: 21 – *Seguridad Física de la red de área local.*

Nivel de Riesgo: 16.67 %

Evaluación del Riesgo: La seguridad física de la red de área local es fuerte. No se detectó ninguna exposición importante.

Categoría del Riesgo: 22 – *Auditoria de la red de área local.*

Nivel de Riesgo: 16.67 %

Evaluación del Riesgo: Las revisiones de auditoria independientes de la red de área local son razonablemente frecuentes.

Categoría del Riesgo: 23 – *Acceso Físico a (Ruteadores).*

Nivel de Riesgo: 16.67 %

Evaluación del Riesgo: Los ruteadores de la red son operados desde ambientes físicamente seguros.

4.4.3.3 Contra medidas

Introducción.

Esta sección incluye la lista de las contra medidas ó salvaguardas y de las recomendaciones que se deben considerar para reducir o eliminar las exposiciones identificadas durante la evaluación. Mientras que el resumen de administración detalla las áreas del sistema que se considera tienen algún riesgo, está parte explica qué se debe hacer para eliminar o para reducir dicho riesgo.

Categoría del Riesgo: *Política y administración de la Seguridad.*

11001 La política corporativa de seguridad debe prohibir específicamente el desarrollo de software no autorizado.

11005 La política corporativa de seguridad debe indicar que el equipo eléctrico debe ser apagado cuando no este uso a menos que haya razones específicas de una unidad o unidades individuales.

11007 El software y los manuales están conforme a la legislación del copyright. El copiado no autorizado de software por algún individuo podía provocar que la organización lleve a cabo un proceso legal. La política corporativa de seguridad debe identificar claramente las acciones que serán tomadas contra el individuo que copia cogido de software ilegalmente.

11008 La política de seguridad corporativa debe incluir la clasificación de los datos, y debe indicar que sus dueños son específicamente responsables de su seguridad.

Categoría del Riesgo: *Acceso a las Instalaciones y datos del Sistema.*

10105 Se debe emplear instalaciones para restringir el acceso a las funciones que los usuarios requieran para sus trabajos.

10106 El acceso al sistema operativo, registro y otras áreas base se deben restringir a los usuarios que son autorizados y experimentados.

10112 Por flexibilidad total, el protector de pantalla debe permitir que el administrador de la seguridad o el usuario defina la acción que debe ser tomada

cuando se activa el mecanismo que es protegido. Idealmente, esto se debe utilizar para prevenir toda entrada/nueva al proceso.

10116 Se debe considerar seriamente la restricción del acceso a las utilidades de gran alcance (tales como aplicaciones de formato del disco).

Categoría del Riesgo: *Seguridad física de activos individuales.*

11429 Las pantallas ó monitores de computadoras deben orientarse para que no muestren datos sensibles por la exhibición hacia ventanas, pasillos públicos, puertas, etc.

11432 El movimiento de activos sensibles (ej. medios magnéticos, reportes, etc.) á y desde la oficina debe ser controlado y registrado estrictamente.

11433 Cuando los activos sensibles (ej. medios magnéticos, reportes, etc.), se transporten, se deben emplear las medidas de seguridad específicas (por ejemplo: cifrado o almacenamiento de datos en cajas fuertes).

Categoría del Riesgo: *Contingencia de la red de área local.*

10950 Los requisitos mínimos de la red de área local, en términos de disponibilidad, funcionamiento y capacidad, deben ser definidos formalmente.
10951 Las instalaciones de contingencia de la red de área local se deben probar por lo menos cada 12 meses.

Categoría del Riesgo: *Instalaciones Criptográficas en la LAN.*

10952 Cuando los datos que pasan sobre la red de área local son de naturaleza confidencial, Se debe considerar la implementación de un mecanismo criptográfico.

10955 Cuando la integridad de datos es esencial, Se debe considerar la aplicación de una técnica de autentificación del mensaje (criptografía).

Categoría del Riesgo: *Control de Cambios.*

104002 Un procedimiento de control de cambios debe asegurar que la implementación de nuevo hardware y software, y los cambios al hardware y al software, han sido autorizados por escrito por la autoridad apropiada.

10403 Todos los cambios planeados deben tener un procedimiento de revocación acordado (debe ser activado en caso de problemas ó errores serios).

10410 Las mejoras de emergencia a los sistemas/componentes críticos deben ser siempre comprobadas/verificadas.

Categoría del Riesgo: *Procedimientos y administración de la auditoria.*

10205 Todos los accesos a programas/funciones sensibles se deben revisar.

10206 Los reportes de auditoria se deben etiquetar con la información pertinente (ej. dueño, fecha producido, etc.).

10209 Las páginas de los reportes de auditoria se deben numerar claramente y deben incluir en un extremo el marcador del informe.

10212 El registro de auditoria debe incluir el nombre del archivo/carpeta/sitio en el que fue registrado para accesarlo (cuando sea apropiado).

Categoría del Riesgo: *Controles y prácticas del cortafuegos.*

70106 Cuando sea práctico, se debe utilizar una aproximación a la ' identidad doble ' en la cuál se utilizan dos tecnologías distintas en la aplicación de cortafuegos para asegurarse que una debilidad explotada en uno no compromete necesariamente al otro.

70115 Los registros de auditoria del cortafuegos deben ser revisados y archivados de forma segura.

70115 Los registros de todas las tentativas de acceso exitosas y no exitosas en el cortafuegos deben ser registradas y revisadas.

Categoría del Riesgo: *Acceso y uso del Internet.*

60101 El Internet se debe utilizar solamente para actividades propias de la organización. La ruptura de esto implica una falta disciplinaria y todos los usuarios deben estar enterados del requerimiento.

60104 Los usuarios deben estar enterados de manera precisa del uso apropiado y eficaz del Internet.

Categoría del Riesgo: *Prácticas de respaldos del Sistema y de datos.*

10306 Si no es práctico realizar respaldos completos diariamente, por lo menos se deben hacer respaldos increméntales diarios, y se deben hacer por lo menos semanalmente los respaldos completos.

103007 Se recomienda que los respaldos completos del sistema se realicen por lo menos semanalmente.

10309 Si es aplicable, los respaldos se deben hacer de los datos de aplicaciones/usuarios así como de los datos/programas del sistema.

10311 Para los sistemas críticos, cuando se realice un respaldo, por lo menos se deben hacer dos copias.

Categoría del Riesgo: *Acceso a los datos sensibles.*

11101 Cuando se elimina un archivo altamente sensible, los datos dentro de ellos deben ser sobre escritos realmente (ej. con ceros binarios).

11105 Para los datos altamente sensibles, el software de seguridad debe asegurarse de que los archivos protegidos puedan accederse solamente por los usuarios específicos o grupos de usuarios.

11106 Para los sistemas informáticos que contienen datos sensibles, se debe utilizar protección lógica y física (ej. una llave de PC, un mecanismo de cerradura).

Categoría del Riesgo: *Control de Acceso y Autenticación.*

11201 Se recomienda que el acceso al sistema/red se bloquee automáticamente por un período de tiempo fijo después de un número consecutivo de intentos de accesos fallidos al sistema.

11208 Cuando se cambia la contraseña de acceso, el sistema de seguridad debe forzar a ingresar la (vieja) contraseña existente para propósitos de validación.

11211 Se recomienda que por lo menos 13 generaciones de contraseña sean almacenadas en el archivo histórico del mecanismo de seguridad.

Categoría del Riesgo: *Acceso Lógico a (Ruteadores).*

12006 El puerto de administración debe ser conectado fuera de banda.

12001 La configuración en línea debe ser deshabilitada.

12013 La contraseña de configuración debe ser cambiada frecuentemente. En muchos casos el cambio mensual es insuficiente.

Categoría del Riesgo: *Mantenimiento de la red de área local.*

10918 El mantenimiento del hardware de la red de área local debe ser programado, y no debe ser realizado mientras que el hardware está siendo utilizando.

Categoría del Riesgo: *Instalaciones Dial-in en la red de área local.*

10920 Se debe desarrollar una política/procedimiento para tener claramente definidos el uso de instalaciones dial-in. Esta debe siempre ser cumplida estrictamente.

10922 Los números de teléfono Dial-in no deben ser iguales, o similares a, los usados por la organización para otros propósitos, a menos que el acceso sea de dominio publico.

10924 Los números de teléfono Dial-in deben ser cambiados si se sospecha de alguna falla de seguridad.

Categoría del Riesgo: *Soporte y Mantenimiento a Ruteadores.*

2096 El trabajo del mantenimiento en los ruteadores de red no se debe realizar mientras estén en uso.

2098 Deben existir acuerdos de respaldos para aprovisionar las fallas de todos los ruteadores críticos de la red.

12002 Los ruteadores primarios de la red no se deben utilizar como dispositivos de respaldos para otros dispositivos primarios.

Categoría del Riesgo: *Detección y administración de Virus.*

10501 Todos los medios movibles (ej. diskettes, CDs) se deben explorar para detectar la posible infección de virus antes de que se utilicen. Esto debe aplicarse sin importar la fuente.

Categoría del Riesgo: *Respaldos y Contingencia.*

10501 Se recomienda que se tomen las medidas necesarias para la adquisición de un sistema ó dispositivo de respaldo si éste llegara a no estar disponible.

Categoría del Riesgo: *Mantenimiento del Hardware.*

10808 Todas las fallas del hardware deben ser completamente documentadas y registradas.

10817 El registro de los activos debe ser revisado periódicamente para asegurarse de que todo el hardware del sistema informático esté considerado.

10820 Para las PC, que tenga fallas como sectores malos y/o perdidos, y cualquier otro error lógico (directorios malos, etc.) que ocurra en el disco duro del sistema informático, deben ser informados al personal de soporte de Pc's. El personal de soporte debe entonces resolver la situación.

Categoría del Riesgo: *Seguridad Física de la red de área local.*

10940 Los cables, las cajas de conexión y otros componentes físicamente expuestos se deben examinar regularmente para detectar intentos no autorizados.

10942 Cuando la confidencialidad de los datos es esencial, se debe considerar la instalación de switches LAN. Esto ayudará a asegurarse de que los paquetes de datos serán vistos solamente por los receptores autorizados.

10943 Los cables y las cajas de conexión no se deben etiquetar físicamente con su función o propósito. Se deben utilizar diagramas indirectos de enumeración/ etiquetado o de configuración para su identificación, y el acceso a éstos debe ser restringido al personal autorizado.

Esta es toda la información que se obtuvo del consultor del riesgo, nuevamente se hace notar que estos resultados son parciales ya que no se incluyen todos los resultados.

4.5 Análisis de Vulnerabilidades de red

4.5.1 Introducción.

Normalmente y en gran mayoría los ataques a las redes corporativas se producen por vulnerabilidades de red dentro de sus servidores, pc´s, host, importantes, y la mayoría son internos, por diferentes tipos de usuarios.

Por tal motivo es esencial e indispensable realizar este tipo de análisis, mismos que nos ayudan a identificar las debilidades existentes, y así poder tomar las acciones necesarias.

Muchos de estos problemas se resuelven únicamente actualizando el software existente con los conocidos parches de seguridad, o modificando alguna configuración.

A continuación se muestra la relación de los Host escaneados.

Relación de todos los host escaneados con la herramienta Nessus, junto con el resultado obtenido, así como su valoración con respecto a: La importancia para el IMP, su Riesgo e Impacto.

En total sé escanearón 224 host, en los cuales se encontraron:

1158 Agujeros de seguridad.
2379 Advertencias de seguridad.
2779 Notas de seguridad.

Esta son las valoraciones que se darán a cada host:

Alto.
Medio.
Bajo.

HOST			Fallas de seguridad	Importancia IMP	Riesgo	Impacto
Nombre	IP Traducida	IP Fuente				
Zami.imp.mx	299.33.186.39	126.2.5.238	(6 Agujeros de seguridad)	Alta	Alta	Alto
cara.imp.mx		192.168.123.6	¿?????	Alta	Alta	Alto
Zamim.imp.mx		126.2.5.238	(16 Agujeros de seguridad)	Alta	Alta	Alto
Zamis.imp.mx	299.33.186.197	126.2.7.72	(11 Agujeros de seguridad)	Alta	Alta	Alto
Inte.imp.mx		192.168.122.162	(5 Agujeros de seguridad)	Alta	Alta	Alto
Inte1.imp.mx		192.168.123.219	(8 Agujeros de seguridad)	Alta	Alta	Alto
bCoat		192.199.189.229	(2 Advertencias de seguridad)	Alta	Alta	Alto
RAS		192.199.189.16	(2 Advertencias de seguridad)	Alta	Alta	Alto
RAS		192.199.189.21	(2 Advertencias de seguridad)	Alta	Alta	Alto
RAS		192.199.189.15	(1 Advertencia de seguridad)	Alta	Alta	Alta
RAS		192.199.189.29	(2 Advertencias de seguridad)	Alta	Alta	Alta
Ras.imp.mx		192.199.189.219	(8 Agujeros de seguridad)	Alta	Alta	Alta
GTI		192.199.189.215	(1 Agujero de seguridad)	Alta	Alta	Alta
RAS		192.199.189.19	(1 Agujero de seguridad)	Alta	Alta	Alta
RAS		192.199.189.18	(1 Agujero de seguridad)	Alta	Alta	Alta
Cicue.imp.mx		192.199.189.298	(5 Agujeros de seguridad)	Medio	Alta	Medio
gtiresn		192.199.189.229	(1 Agujero de seguridad)	Medio	Alta	Bajo
RAS		192.199.189.17	(2 Agujeros de seguridad)	Medio	Alta	Bajo
Root.imp.mx		192.199.181.192	(1 Agujero de seguridad)	Medio	Alta	Medio
Gltii.imp.mx		192.199.181.35	(11 Agujeros de seguridad)	Medio	Alta	Medio
fghj		192.199.181.32	(4 Agujeros de seguridad)	Medio	Alta	Medio
Vimus.imp.mx		192.199.181.5	(8 Agujeros de seguridad)	Medio	Medio	Medio

Abal.imp.mx		192.199.181.196	(7 Agujeros de seguridad)	Medio	Medio	Medio
Gtilib.imp.mx		192.199.181.87	(7 Agujeros de seguridad)	Medio	Medio	Medio
Gtilibe.imp.mx		192.199.181.2	(19 Agujeros de seguridad)	Medio	Medio	Medio
Venuseting.imp.mx		192.199.181.28	(9 Agujeros de seguridad)	Medio	Medio	Medio
uut.imp.mx		192.199.181.86	(20 Agujeros de seguridad)	Medio	Medio	Bajo
matz.imp.mx		192.199.181.229	(8 Agujeros de seguridad)	Medio	Medio	Medio
Inte7.imp.mx		192.168.123.197	(6 Agujeros de seguridad)	Medio	Medio	Medio
Inte1.imp.mx		192.168.123.198	(6 Agujeros de seguridad)	Medio	Medio	Medio
Inte6.imp.mx		192.168.123.199	(6 Agujeros de seguridad)	Medio	Medio	Medio
Inte3.imp.mx		192.168.123.299	(7 Agujeros de seguridad)	Medio	Medio	Medio
Inters.imp.mx		192.168.123.292	(1 Agujero de seguridad)	Medio	Medio	Medio
casara.imp.mx		192.168.123.293	¿??????	Medio	Medio	Medio
Porta.imp.mx		192.168.123.299	¿??????	Medio	Medio	Medio
Inte58.imp.mx		192.168.123.219	¿??????	Medio	Medio	Medio
		192.168.125.216	(4 Agujeros de seguridad)	Bajo	Bajo	Bajo
IS		192.168.122.2	(10 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.152.221	(7 Agujeros de seguridad)	Bajo	Bajo	Bajo
IS~5		192.168.122.19	(6 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.219	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.152.82	(21 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.237	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.125.73	(21 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.226	(4 notas de seguridad)	Bajo	Bajo	Bajo
		192.168.122.132	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.122.215	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.253	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.292	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.125.119	(7 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.137	(1 Agujero de	Bajo	Bajo	Bajo

			seguridad)			
		192.168.122.229	(7 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.18	(6 Agujeros de seguridad)	Bajo	Bajo	Bajo
ACEITE		192.168.152.56	(28 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.152.162	(4 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.152.225	(7 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.131	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.152.212	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.252	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.12	(21 Agujeros de seguridad)	Bajo	Bajo	Bajo
.lola.imp.mx		192.168.152.221	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.125.219	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.17	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
Mimo.imp.mx		192.168.125.55	(7 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.152.226	(3 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.152.112	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.152.235	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.122.222	(6 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.22	(3 Agujeros de seguridad)	Bajo	Bajo	Bajo
h.imp.mx		192.168.152.69	(11 Agujeros de seguridad)	Medio	Bajo	Bajo
		192.168.125.213	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.119	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.152.11	(6 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.218	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.122	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.122.113	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.125.192	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.125.129	(1 Agujero de seguridad)	Bajo	Bajo	Bajo

		192.168.122.223	(7 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.212	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.259	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
SARAR		192.168.125.239	(4 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.19	(11 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.197	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.152.217	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.23	(11 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.123	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.125.89	(3 advertencias de seguridad)	Bajo	Bajo	Bajo
		192.168.152.222	(7 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.125.128	(1 Agujero de seguridad)	Bajo	Bajo	Bajo
		192.168.152.229	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.211	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.122.85	(7 Agujeros de seguridad)	Bajo	Bajo	Bajo
		192.168.152.196	(2 Agujeros de seguridad)	Bajo	Bajo	Bajo

Por razones de seguridad para el Instituto Mexicano del Petróleo se alteraron las direcciones IP y no se incluirá el reporte detallado de las vulnerabilidades encontradas.

4.6 POLÍTICAS DE SEGURIDAD

4.6.2 Pasos para la implementación

En este proceso se mencionan 6 pasos los cuales se mencionan a continuación:

1.- El primer paso es imprimir las políticas de la seguridad de la información de esté documento.
2.- El segundo paso es estudiar las políticas.
3.- El tercero es la revisión y adecuación de las políticas a la organización.
4.- El cuarto es la confirmación y la ratificación de las políticas.
5.- El quinto es la publicación de las políticas.
6.- El sexto es la implementación y el cumplimiento con las políticas.

4.6.3 Políticas de seguridad para el Instituto Mexicano del Petróleo

Estas políticas se obtuvieron con relación al resultado obtenido en el Análisis de Riesgos en la parte del incumplimiento con el ISO17799-1.

A continuación se mostrarán un conjunto parcial de las políticas que se deben revisar en el Laboratorio de TI. Para su posible implementación, dichas políticas fueron obtenidas de la herramienta RUsecure.

Planeación de la continuidad del negocio.
11.1.1

Política 080101. Iniciar el proyecto de BCP.
Requiere la gerencia iniciar un plan de la continuidad del negocio.

Política 120303. Plan de Recuperación de Desastres.
Los dueños de los sistemas de información de la organización deben asegurarse de que los planes de recuperación de desastre para sus sistemas estén desarrollados, probados, e implementados.

Seguridad del personal.
6.1.1

Política 090101. Preparación de términos y de condiciones de *empleo.*
Los términos y las condiciones de empleo de esta organización son incluir los requisitos para la conformidad con la seguridad de la información.

Política 090110. Responsabilidad de los empleados de proteger la confidencialidad de datos.
Requerir a todos los empleados firmar un documento formal referente a la necesidad de proteger la confidencialidad de la información, durante y después de relaciones contractuales con la organización.

Política 090108. Cumplimiento con la política de la seguridad de la información.
Todos los empleados deben conformarse con las políticas de seguridad de información de la organización. Cualquier incidente de la seguridad de la información que resulte del incumplimiento dará lugar a la acción disciplinaria inmediata.

Cumplimiento.
12.1.1

Política 070101. Estando enterado de obligaciones legales.
Las personas responsables de la gerencia de recursos humanos deben asegurarse de que todos los empleados están completamente enterados de sus responsabilidades legales con respecto al uso de los sistemas de información y de

los datos computarizados. Tales responsabilidades deben ser incluidas dentro de la documentación principal del personal tal como términos y condiciones del empleo y del código de conducta de la organización.

Política 070404. Grabación de las Conversaciones por Teléfono.
Todas las partes deben ser notificadas por adelantado siempre que se estén registrando las conversaciones.

Política 070302. Uso la información con derechos de autor de Internet.
La información del Internet o de otras fuentes electrónicas no se puede utilizar sin la autorización del dueño.

Política 070403. Asegurando los Riesgos.
Una nueva evaluación de las amenazas y de los riesgos implicados referentes a las actividades económicas de la organización debe realizarse periódicamente para asegurarse de que la organización está asegurada adecuadamente.

Clasificación y control de activos.
5.1.1

Política 010601. Manejo y uso de la documentación del hardware.
La documentación del hardware se debe guardar actualizada y fácilmente disponible para el personal autorizado a dar soporte y mantenimiento a los sistemas.

Política 010602. Mantener un inventario o un registro del hardware.
Un inventario formal del hardware de todo el equipo debe estar siempre actualizado y mantenido constantemente.

Política 030801. Usar Técnicas de Cifrado.
Cuando sea apropiado, la información o los datos sensibles o confidenciales se debe transmitir siempre en forma cifrada. Antes de la transmisión, se debe tomar en consideración siempre los procedimientos que se utilizarán entre el emisor y las partes receptoras y cualquier cuestión legal posible con respecto al uso de técnicas de cifrado.

Política 030802. Compartir la Información.
Las personas responsables de la administración de recursos humanos deben asegurarse de que todos los empleados están completamente enterados de sus deberes y responsabilidades legales y corporativos referentes a la inadecuada compartición de la información, internamente dentro de la organización y a las partes externas.

Seguridad de la Organización.
4.1.2

Política 030201. Nombrar a Administradores de Sistemas.

Los sistemas de la organización deben ser manejados por un administrador de sistemas convenientemente calificado que sea responsable de supervisar el funcionamiento y la seguridad cotidianas de los sistemas.

Política 030202. Sistemas de Administración.
Los administradores de sistema deben estar completamente entrenados y tener la experiencia adecuada en la amplia gama de sistemas y de las plataformas usados por la organización. Además, debe estar bien informado y consiente con respecto a la gama de riesgos de la seguridad de la información que necesitan ser administrados.

Política 060108. Manipulación de Advertencias de Virus y Hoax.
Los procedimientos a emplearse en las advertencias del virus y de hoax deben estar implementados y mantenidos.

Sistemas de Control de Accesos.
9.1.1

Política 030301. Descargar archivos e información de Internet.
Se debe tener mucho cuidado al descargar información y archivos de Internet para proteger contra código malicioso y contra material inadecuado.

Política 030312. Uso del Internet para los propósitos del trabajo.
La gerencia es responsable de controlar el acceso del usuario al Internet, así como para asegurarse de que los usuarios están enterados de las amenazas, y capacitados en las salvaguardas, para reducir el riesgo de los incidentes de la seguridad de la información.

Política 030516. Compartir datos en sistemas de administración de proyectos.
Solamente las personas autorizadas pueden tener acceso a los datos sensibles o confidenciales sobre los proyectos contenidos o manejados por la organización o sus empleados.

Política 030810. Protección de Documentos con Contraseñas.
Los datos electrónicos y la información sensibles/confidenciales deben ser asegurados, siempre que sea posible, con la aplicación de controles de acceso al directorio (de la computadora) en el sistema concerniente. El solo uso de contraseñas para asegurar documentos individuales es menos eficaz, y por lo tanto no recomendado, pues las contraseñas pueden ser olvidadas o revelarse (en un cierto plazo) a personas no autorizadas.

Administración de Operaciones y Equipo de Cómputo.
8.1.1

Política 030209. Programar la Operación de Sistemas.
Los horarios de operación de los sistemas deben ser planeados, autorizados y documentados formalmente.

Política 030210. Programar los cambios a las rutinarias de operación de los sistemas.
Los cambios a las rutinarias de operación de los sistemas deben ser probados y aprobados completamente antes de ser implementados.

Política 060106. Salvaguardar contra ataques de denegación de servicio.
Los planes de contingencia para un ataque de denegación de servicio deben ser mantenido y ser probada periódicamente para asegurar su eficacia.

Política 060110. Respondiendo a los incidentes de virus.
La amenaza presentada por la infiltración de un virus es alta, al igual que el riesgo a los archivos y datos de los sistemas de la organización. Los procedimientos formales para responder a un incidente del virus deben ser desarrollados, probados e implementados. La respuesta a incidentes del virus debe ser revisada y probada regularmente.

Desarrollo y Mantenimiento de Sistemas.
10.1.1

Política 040204. Software de Interconexión de Aplicaciones/Sistemas.
Desarrollar el software sistemas de interconexión es una tarea altamente técnica y se debe emprender solamente de una manera planeada y controlada por el personal correctamente calificado.

Política 030303. Envío de Correo Electrónico (E-mail).
El correo electrónico se debe utilizar solamente para los propósitos del negocio, usando los términos que son consistentes con otras formas de comunicación del negocio. Los archivos de datos adjuntos a un correo electrónico se permiten solamente después de confirmar la clasificación de la información que es enviada y después que se explora y verifica el archivo de la posibilidad de que contengan virus ó de otro código malicioso.

Política 030304. Recepción de Correo Electrónico (E-mail).
El correo electrónico entrante se debe tratar con extremo cuidado debido a sus riesgos inherentes de la seguridad de la información. La abertura del correo electrónico con archivos adjuntos no se permite a menos que tales archivos se hayan examinado contra el posible contenido de virus ú otro código malicioso.

Política 030206. Manejo de operaciones del sistema y administración de sistema.
Los sistemas de la organización se deben operar y administrar usando procedimientos documentados de manera que sea eficiente pero también eficaz en la protección de la seguridad de la información de la organización.

Política 030207. Documentación del Manejo del Sistema.
La documentación del sistema es un requisito para todos los sistemas de información de la organización. Tal documentación de debe mantener actualizada y estar disponible.

Seguridad Física y Ambiental.
7.1.1

Política 120202. Manejo de Almacenes de Datos remotos.
Los sitios remotos en donde se almacenan los datos deben proporcionar los controles y la protección de acceso que reducen el riesgo de la pérdida o del daño a un nivel aceptable.

Política 120104. Control de acceso físico a las áreas seguras.
Todas las premisas de la computadora se deben proteger contra el acceso no autorizado usando un equilibrio apropiado entre las simples medidas de identificación, hasta tecnologías más complejas para identificar, autenticar y supervisan todas las tentativas de acceso.

Política 010503. Usar Gabinetes de Almacenamiento Protegidos contra Fuego.
Los documentos deben ser almacenados de manera segura de acuerdo con su estado de clasificación.

Política 010504. Usar una caja fuerte.
Los documentos deben ser almacenados en una manera segura de acuerdo con su estado de clasificación.

Política 030806. Riesgos de fuego en la información.
Todos los datos e información se deben proteger siempre contra el riesgo de daño por fuego. El nivel de tal protección debe reflejar siempre el riesgo de fuego, el valor y la clasificación de la información que es salvaguardada.

Este seria el final del análisis de riesgos dentro del Laboratorio de TI., Lo siguiente es analizar los resultados obtenidos en dicho análisis y manejarlos, este trabajo debe de ser realizado por todo el personal que involucra este análisis.

5 RESULTADOS Y CONCLUSIONES

A continuación se mostrarán los resultados obtenidos en forma de tablas.

5.1 Políticas y controles

Esta tabla nos muestra cada uno de los tópicos del ISO17799-1, el número de controles recomendados por el BS7799-2 y las políticas que esto generó con base en el RUsecure.

Tópico.	Controles.	Políticas.
Planeación de la continuidad del negocio.	1	2
Seguridad del personal.	9	47
Cumplimiento.	11	54
Clasificación y control de activos.	3	16
Seguridad de la organización.	8	23
Políticas de seguridad.	2	0
Sistemas de control de acceso.	19	47
Administración de operaciones y equipo de cómputo.	17	68
Desarrollo y mantenimiento de sistemas.	11	37
Seguridad física y ambiental.	9	31
Total	90	325

Tabla 5.1

Las siguientes son definiciones que nos ayudan a poder interpretar los resultados mostrados en las siguientes tablas.

Con respecto a los Riesgos:

ALTO – Afecta a recursos críticos de la organización, por lo que debe ser solucionado el problema de inmediato.

MEDIO – Afecta recursos importantes de la organización, pero los procesos críticos del negocio se mantienen sin ser afectados (por lo menos durante un tiempo razonable). Se requiere actualizar los sistemas pero no es necesario distraer recursos para hacerlo de inmediato (hay tiempo para planear).

BAJO – Afecta sistemas no críticos para la organización, Se pueden actualizar los sistemas cuando la carga de trabajo sea menor para no afectar la operación, actualización no prioritaria).

Con respecto a los Impactos:

Substancial - Podría ser crítico, estimado en más de $1 millón.

Severo - Estimado en más de $ 1 millón.

Considerable - Estimado está de $100.000 a $1 millón.

Significativa - Estimado en el rango de $10.000 a $100.000).

Importantes - Estimado para estar en el rango de $10.000 a $100.000.

Mensurable pero no crítica - Estimado de $1.000 y $10.000.

Limitada - Se considera de $1.000 a $10.000.

Alto = Urgente = Substancial.
Medio = Inmediato = Significativo.
Bajo = Corto plazo = limitado.

5.2 Consultor del Riesgo.

5.2.1 Tabla de los resultados obtenidos del cuestionario *A 01* de la evaluación del alto riesgo

5.2 En esta tabla se muestran las áreas identificadas en las cuales se juzga que requieren una atención inmediata, y para las cuáles puede ser requerida una evaluación detallada.

Pérdida de	Riesgo.			Impacto.		
Disponibilidad	64.33 %	Alto	Urgente.	100 %	Alto	substancial
Confidencialidad	60.27 %	Alto	Inmediato	100 %	Alto	significativo
Integridad	59.19 %	Alto	corto plazo	100 %	Alto	significativo
Negocio		Alto	Urgente.	100 %	Alto	substancial

Tabla 5.2

5.2.2 Tabla de los resultados obtenidos de cuestionario *A 02 de la evaluación del Riesgo de la Seguridad de TI.*

5.3 En esta tabla se muestran las áreas identificadas en la evaluación de riesgos de la seguridad de TI. Se encontró que existen varias exposiciones con un nivel de riesgo e impacto alto, por lo cual se deben revisar urgentemente, también es necesario realizar un análisis detallado para cada área mencionada.

Tópico.	Riesgo.		
Conocimiento General de la Seguridad	Alto	89.29 %	Substancial
Prácticas de administración de la Seguridad	Alto	75.00 %	Substancial
Política de Seguridad – Contenido	Alto	67.31 %	Significativo
Operación de Sistemas y Componentes de auditoria	Alto	66.67 %	Substancial
Política de Seguridad – Alcance.	Medio	52.63 %	Significativo
Operación de Sistemas y Componentes del Sistema	Alto	42.86 %	Significativo
Consideraciones Relacionadas al Negocio: Los datos son relativamente sensibles y confidenciales, con impacto financiero mensurable. La pérdida potencial máxima por actividad fraudulenta es significativa de $10.000 a $100.000. La pérdida potencial máxima por modificación no autorizada de datos es limitada de $1.000 y $10.000.			

Tabla 5.3

5.4 Esta tabla muestra los impactos potenciales que podrían resultar de las exposiciones identificadas, en la tabla anterior.

Tópico.	Impacto.		
Pérdida por Indisponibilidad del Sistema.	Alto	100 %	Substancial
Indisponibilidad – Tiempo Critico.	Alto	80.63 %	Severo
Pérdida Financiera por error de Funcionamiento.	Alto	70.53 %	Considerable
Reemplazo y reconstrucción del Equipo.	Alto	69.47 %	Considerable
Costo del reemplazo de Datos, Software, etc.	Medio	60.95 %	Significativo
Sensibilidad y confidencialidad de los Datos.	Medio	50.53 %	Importante
Fraude Potencial.	Medio	50.53 %	Significativa
Costo de Reemplazo y capacitación del Personal.	Medio	50.53 %	Considerable
Reemplazo del Equipo.	Medio	40.00 %	Importante
Indisponibilidad: acción civil legal.	Bajo	33.33 %	Limitado
Indisponibilidad – Confianza del Mercado.	Medio	33.33 %	Importante
Indisponibilidad: Visibilidad/Reputación.	Bajo	33.33 %	Limitado
Pérdida del cliente por Indisponibilidad.	Bajo	33.33 %	Limitado
Modificación no autorizada de Datos.	Bajo	30.53 %	Limitado
Pérdida financiera por error de Software.	Bajo	30.53 %	Limitado
Sistemas Dependientes.	Bajo	7.42 %	Limitado
Implicaciones Reguladoras por Indisponibilidad	Bajo	30.53 %	Limitado

Tabla 5.4

5.2.3 Tabla de los resultados obtenidos del cuestionario *D 01 Evaluación del riesgo de la infraestructura de la seguridad electrónica.*

5.5 En esta tabla se muestra el resultado producto del análisis de riesgos en la Infraestructura de Seguridad Electrónica del IMP, se encuentran las áreas que necesitan atención, aunado a un porcentaje donde entre más alto es el porcentaje mayor será el impacto.

Tópico.	Riesgo		
1- Política y administración de la Seguridad	Alto	88.18 %	Substancial
2 - Acceso a las instalaciones y datos del Sistema.	Alto	77.50 %	Significativo
3 - Seguridad física de activos individuales	Alto	77.50 %	Significativo
4 - Contingencia de la red de área local.	Alto	75.00 %	Urgente
5 - Instalaciones Criptográficas en la LAN.	Alto	70.83 %	Importante
6 – Control de Cambios.	Alto	68.75 %	Importante
7 – Procedimiento y administración de auditoria	Medio	62.50 %	Importante
8 – Controles y prácticas del cortafuegos	Alto	62.50 %	Significativo
9 – Acceso y uso de Internet	Medio	61.11 %	Importante
10 – Prácticas de respaldos del Sistema y de datos	Medio	59.09 %	Importante
11 – Acceso a los datos sensibles	Medio	57.14 %	Importante
12 – Control de acceso y autenticación	Medio	56.90 %	Importante
13 – Acceso Lógico a (Ruteadores)	Bajo	56.00 %	Limitado
14 – Mantenimiento de la red de área local.	Bajo	55.00 %	corto plazo
15 – Instalaciones Dial-in en la red de área local.	Medio	53.06 %	Importante
16 – Soporte y Mantenimiento de ruteadores.	Bajo	50.00 %	corto plazo
17 – Detección y administración del Virus.	Medio	50.00 %	importante
18 – Administración de la red de área local.	Bajo	37.50 %	Limitado
19 – Respaldos y Contingencias.	Bajo	25.00 %	Limitado
20 – Mantenimiento del Hardware.	Bajo	23.13 %	Limitado
21 – Seguridad Física de la red de área local.	Bajo	16.67 %	Nada
22 – Auditoria de la red de área local.	Bajo	16.67 %	Nada
23 – Acceso Físico a (Ruteadores).	Bajo	16.67 %	Nada

Tabla 5.5

5.3 CONCLUSIONES.

La manera más efectiva de dar seguridad a la información es seguir una metodología estructurada basada en los propios requerimientos del IMP.

El estándar BSS7799, ahora ISO 17799 ayuda a implementar "mejores prácticas" en la administración de la seguridad de la información. Sus objetivos son proveer a las empresas e instituciones como el IMP de bases para proteger la información aún cuando esta tenga que ser compartida con terceros.

En este nuevo marco se hace énfasis no solo en reaccionar cuando algún incidente ya sucedió sino a evaluar los riesgos a los cuales estamos expuestos y tratar de atenuar las consecuencias cuando estos sucedan, se hace especial énfasis en los papeles y responsabilidades de seguridad informática del personal dentro de la empresas y se sugiere una estructura administrativa dirigida por un Oficial de Seguridad en jefe apoyado por oficiales de seguridad asociados con los principales recursos informáticos de la empresa (bases de datos, redes, servidores, infraestructura, desarrollo de aplicaciones, etc.).

Es solo hasta que se haya definido una primera estructura administrativa, que se debe pasar al diseño de la arquitectura de seguridad a implementar en la Institución. Para su diseño es necesario primero conocer lo que se va a proteger (conocimiento que normalmente posee el dueño de la información o del recurso) y cual será el costo por brindar esa protección. Para obtener toda esta información se usan herramientas como lo son los análisis de riesgos, análisis de vulnerabilidades, etc.

El IMP en realidad ya cuenta con una primera arquitectura de seguridad la cual fue resultado de una "evaluación de la seguridad" realizado en el año 2000, por lo que deberá ponerse énfasis en análisis de este tipo para ver si la arquitectura actual de seguridad es suficiente o si es necesario mejorarla y esto resulta costeable.

Los resultados de este trabajo, aunque parciales por haber sido obtenidos de cuestionarios aplicados solo a personal del Laboratorio de TI, pueden ser extrapolados fácilmente a todo el Instituto Mexicano del Petróleo.

En lo que se refiere a la alineación con respecto a la norma, lo primero que resaltan los resultados es la falta de una estructura institucional para la administración de la seguridad, la falta o actualización de una política de seguridad institucional, la falta de una definición clara de los roles de seguridad que debe jugar cada empleado, la falta de cultura en seguridad en el IMP.

La seguridad informática aún no ha perneado de manera adecuada en nuestro Instituto. La desviación que existe con respecto a la norma no es infranqueable, pero implica una buena cantidad de trabajo a realizar.

Muchos de los equipos analizados presentan huecos de seguridad por falta de una buena configuración, por servicios levantados sin necesidad y por falta de una

aplicación sistemática de parches, cabe mencionarse que esto debe solucionarse rápidamente.

5.4 Recomendaciones de cómo atacar estos resultados.

Con respecto al Análisis de Vulnerabilidades de red.

Esta tabla muestra los Host más significativos del IMP, junto con una valoración respecto a su importancia, riesgo e impacto para el IMP, dadas las vulnerabilidades encontradas, es necesario tomar las medidas necesarias urgentemente para contrarrestarlas, ya que los servicios proporcionados por estos host son de vital importancia. Lo primero que se recomienda es eliminar las vulnerabilidades encontradas.

También se hace notar que para causas de publicación en esta tesis por seguridad del IMP. Se modificaron los nombres y las direcciones IP de todos los host mencionados en esta tesis.

HOST	IP Traducida	IP Fuente	Fallas de seguridad	Importancia IMP	Riesgo	Impacto
Gesndnam.imp.mx	200.2.16.0	192.5.5.8	(8 Agujeros de seguridad)	Alta	Medio	Media
Rtfeaami.imp.mx		192.6.4.6	(6 Agujeros de seguridad)	Alta	Alta	Alto
Ararrmil.imp.mx	200.1.86.7	192.4.7.9	(11 Agujeros de seguridad)	Alta	Medio	Medio
Cacauiei.imp.mx		192.4.1.1	(5 Agujeros de seguridad)	Alta	Alta	Alto
Ibcynssa.imp.mx		192.1.1.10	(8 Agujeros de seguridad)	Alta	Alta	Alto
Aaipappe.imp.mx		192.1.1.50	(2 Advertencias de seguridad)	Alta	Medio	Bajo
Sooosaon.imp.mx		192.1.11.2	(8 Agujeros de seguridad)	Alto	Medio	Medio
Dynradsg.imp.mx		192.1.11.7	(9 Agujeros de seguridad)	Alto	Alto	Medio
Ipqptrae.imp.mx		192.1.1.8	(20 Agujeros de seguridad)	Alto	Alto	Alto
Oouoieyn.imp.mx		192.1.1.13	(6 Agujeros de seguridad)	Alto	Medio	Medio
Sredssae.imp.mx		192.1.1.19	(6 Agujeros de seguridad)	Alto	Medio	Medio
Pleefar.imp.mx		192.1.1.99	(6 Agujeros de seguridad)	Alto	Medio	Medio
Oasramia.imp.mx		192.1.1.20	(7 Agujeros de seguridad)	Alto	Medio	Medio

Rstlcifl.imp.mx		192.1.1.05	(1 Agujero de seguridad)	Alto	Medio	Medio
Eaoeciau.imp.mx		192.1.1.23	(3 Agujero de seguridad)	Alto	Medio	Medio
Stgsijmt.imp.mx		192.1.1.69	(28 Agujeros de seguridad)	Alto	Medio	Medio
Tiedoar.imp.mx		192.1.1.254	(7 Agujeros de seguridad)	Alto	Medio	Medio

Con respectó a los resultados obtenidos para el **cumplimiento con la norma ISO17799:**

En forma de importancia.

Lo primero que recomendaría sería para el punto de la **Seguridad de la Organización** la creación de lo siguiente:

4.1.1 **Foro gerencial sobre seguridad de la información.** Debe tenerse en cuenta la creación de un foro gerencial para garantizar que existe una clara dirección y un apoyo manifiesto de la Dirección a las iniciativas de seguridad.

4.1.2 **Coordinación de la segundad de la información.** En una gran organización podría ser necesaria la creación de un foro ínter funcional que comprenda representantes gerenciales de sectores relevantes de la organización para coordinar la implementación de los controles de seguridad de la información.

Después planear en base al punto de **Plantación de la Continuidad del Negocio** un:

11.1.1 **Proceso de administración de la continuidad del negocio**.
Se debe implementar un proceso controlado para el desarrollo y mantenimiento de la continuidad del negocio en toda la organización.

Seguido de esto realizar en base al punto de **Políticas de seguridad** y tomando como referencia las políticas generadas por el Rusecure:

3.1.1 **Documentación de la política de seguridad de la información.** Los responsables del nivel gerencial deberán aprobar y publicar un documento que contenga la política de seguridad y comunicarlo a todos los empleados, según corresponda.

En base al punto del **Cumplimiento** realizar lo siguiente:

12.1.1 **Identificación de la legislación aplicable.** Se deben definir y documentar claramente todos los requisitos legales, normativos y contractuales pertinentes para cada sistema de información.

12.2.1 **Cumplimiento de la política de segundad.** La gerencia debe garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad. Asimismo, se debe considerar la implementación de una revisión periódica de todas las áreas de la organización para garantizar el cumplimiento de las políticas y estándares de seguridad.

En base a la **Clasificación y control de activos**:

5.1.1 **Inventario de activos.** Un inventario de todos los activos importantes será redactado y mantenido.

5.1.2 **Pautas de clasificación.** Las clasificaciones y controles de protección asociados a la información, deben tomar cuenta de las necesidades de la empresa con respecto a la distribución o restricción de la información, y de la incidencia de dichas necesidades en las actividades de la organización.

Otra de las más importantes es la **Segundad del Personal** por lo cual tendrían que realizarse las acciones siguientes:

6.2.1 **Formación y capacitación en materia de seguridad de la información.** Todos los empleados de la organización y cuando sea pertinente, todos los usuarios externos, deben recibir una adecuada capacitación y actualizaciones periódicas en materia de políticas y procedimientos de seguridad de la organización.

6.1.1 **Inclusión de la seguridad en las responsabilidades de los puestos de trabajo.** Las funciones y responsabilidades en materia de seguridad, según consta en la política de seguridad dé la información de la organización (ver 3.1), deben ser documentadas según corresponda.

6.1.2 **Selección y política de personal.** Se deben llevar a cabo controles de verificación del personal permanente en el momento en que se solicita el puesto.

6.1 3 **Acuerdos de confidencialidad.** Los empleados deben firmar habitualmente un acuerdo de confidencialidad como parte de sus términos y condiciones iniciales de empleo.

6.3.1 **Comunicación de incidentes relativos a la seguridad.** Los incidentes relativos a la seguridad deben comunicarse a través de canales gerenciales apropiados tan pronto como sea posible.

6.3.2 **Comunicación de debilidades en materia de seguridad.** Los usuarios de servicios de información deben advertir, registrar y comunicar las debilidades o amenazas supuestas u observadas en materia de seguridad, con relación a los sistemas o servicios.

6.3.5 **Proceso disciplinario.** Debe existir un proceso disciplinario formal para los empleados que violen las políticas y procedimientos de seguridad de la organización.

Con respecto a los **Sistemas de control de acceso**:

9.1.1 **Política de control de accesos.** Se deben definir y documentar los requerimientos de negocio para el control de accesos. Las reglas y derechos del control de accesos para cada usuario o grupo de usuarios deben ser claramente establecidos en una declaración de política de accesos.

Con respectos a la **Administración de operaciones y equipo de cómputo**:

8.1 .1 **Documentación de los procedimientos operativos.** Se deben documentar y mantener los procedimientos operativos identificados en la política de seguridad en 4.1.1.1

8.1.2 **Control de cambios en las operaciones.** Se deben controlar los cambios en los sistemas e instalaciones de procesamiento de información.

Con respecto al **Desarrollo y mantenimiento de sistemas**:

10.1.1 **Análisis y especificaciones de requerimientos de la seguridad.** Los requerimientos del negocio para los sistemas nuevos, o las mejoras a los sistemas existentes especificarán los requerimientos para los controles.

10.3.1 **Política en el uso de controles criptográficos.** Se desarrollara y seguirá una política para el uso de los controles criptográficos para la protección de la información.

Con respecto a la **Seguridad física y ambiental**:

7.1.1 **Perímetro de seguridad física.** Las organizaciones deben utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información crítica o sensible.

7.1.4 **Desarrollo de tareas en áreas protegidas.** Controles y herramientas adicionales para el desarrollo de las tareas en áreas aseguradas deben ser usados para incrementar la seguridad dada por la protección de los controles físicos del área protegida.

Con respecto a los resultados obtenidos de ***A02 Evaluación del nesgo da la Seguridad de Tecnologías de la Información.***

En orden de importancia:

Categoría del Riesgo: *Conocimiento General de la Seguridad.*

El nivel del conocimiento de la seguridad es bajo, con un correspondiente aumento en el riesgo de problemas de seguridad. Esto se debe tratar rápidamente con nuevas iniciativas y medidas adicionales.

Contramedidas:

- Todo el personal nuevo debe ser informado de las políticas y estándares de seguridad y de sus propias responsabilidades con respecto a esto.
- Los empleados deben ser instruidos para enfrentar a visitantes desconocidos, y llevarlos a recepción o al lugar donde deben estar.
- Los usuarios deben ser informados que serían responsables por las pérdidas resultando del acceso de contraseñas confidenciales.
- Se debe iniciar un programa para mejorar el conocimiento de la seguridad.

Esto puede incluir seminarios/cursos, boletines de noticias de la seguridad, etc.

Categoría del Riesgo: *Prácticas de la administración de la Segundad.*

Las prácticas de administración de la seguridad esta por debajo del estándar y no mantiene controles de segundad.

Contramedidas:

La política de la seguridad es de poco valor si no se hace cumplir realmente. La aplicación forzosa de la política debe ser primordial y todos los mecanismos de seguridad deben estar activados.

A todos los recursos se les debe asignar un dueño específico, incluso si éste no es realmente el responsable actual. El dueño debe estar requerido para especificar un nivel de protección.

La responsabilidad de coordinación de la seguridad debe ser asignada específicamente.

Categoría del Riesgo: *Política de Segundad— Contenido.*

La política es pobre en varias áreas importantes. Las omisiones pueden aumentar algunos riesgos. La política deb3 ser realzada más a fondo.

Contramedidas:

Todos los sistemas deben estar completamente y adecuadamente asegurados. Se debe incluir la disposición por la perdida física del equipo y la pérdida consecuente debido a la indisponibilidad funcional.

Para las instalaciones sensibles, la publicidad y los viajes innecesarios deben ser evitados.

Un índice de toda la información sensible impresa debe ser mantenido. Debe incluir información tal como: l nivel de seguridad de cada documento, su destino, etc.

Todos los recursos de los datos deben tener un nivel o una etiqueta de seguridad.

Esto se podría utilizar para restringir el acceso y/o para identificar sensibilidad relativa.

Categoría del Riesgo: *Política de Seguridad relacionada al Personal.*

Contramedidas:

Una cláusula detallando las responsabilidades de seguridad debe ser incluida en todos los contratos de todos los vendedores/surtidores que tengan acceso a los datos, a los recursos o a las premisas de la organización.

Una cláusula detallando las responsabilidades de segundad debe ser incluida en los contratos de todos los ingenieros y personal de mantenimiento.

La política de la seguridad debe prohibir específicamente el almacenamiento de contraseñas de, terminales con funciones importantes en discos con programas de conexión automática.

Donde es posible se debe usar software para restringir el uso no autorizado de los recursos.

Con respecto a los resultados obtenidos de ***D01 Evaluación del riesgo de la infraestructura de la seguridad electrónica.***

En orden de importancia:

Categoría del Riesgo: *Política y administración de la Seguridad.*

Evaluación del Riesgo: La política de seguridad es incomprensible, no esta completa y las practicas de administración de la seguridad está en carencia. Es probable que esto tenga un efecto perjudicial en el nivel de seguridad en un número de áreas, aumentando el riesgo. Es esencial tomar acción sobre esto.

Contramedidas:

11001 La política corporativa de seguridad debe prohibir específicamente el desarrollo de software no autorizado.

11008 La política de seguridad corporativa debe incluir la clasificación de los datos, y debe indicar que sus dueños son específicamente responsables de su seguridad.

11005 La política corporativa de seguridad debe indicar que el equipo eléctrico debe ser apagado cuando no este uso a menos que haya razones específicas de una unidad o unidades individuales.

11007 El software y los manuales están conforme a la legislación del copyright. El copiado no autorizado de software por algún individuo podía provocar que la organización lleve a cabo un proceso legal. La política corporativa de seguridad debe identificar claramente las acciones que serán tomadas contra el individuo que copia cogido de software ilegalmente.

Categoría del Riesgo: *Acceso a las instalaciones y datos del Sistema.*

Evaluación del Riesgo: Los mecanismos de seguridad en el sistema son relativamente débiles. El acceso a las instalaciones y a los datos del sistema se controla inadecuadamente. Se requiere una revisión.

Contramedidas:

10105 Se debe emplear aplicaciones para restringir el acceso a los recursos que los usuarios necesiten para realizar su trabajo.

10106 El acceso al sistema operativo, registros y otras áreas base se deben restringir a los usuarios autorizados y experimentados.

10112 Por flexibilidad total, el protector de pantalla debe permitir que el administrador de la seguridad o el usuario defina la acción que debe ser tomada cuando se activa el mecanismo de protección. Idealmente, esto se debe utilizar para prevenir toda entrada nueva al proceso.

10116 Se debe considerar seriamente la restricción del acceso a las aplicaciones de gran alcance (tales como aplicaciones de formato del disco).

Categoría del Riesgo: *Seguridad física de activos individuales.*

Evaluación del Riesgo: La protección física de acceso a los activos individuales (medios, informes, etc.) es pobre. Los procedimientos y las prácticas no reflejan las amenazas planteadas. Se requieren controles más fuertes.

Contramedidas:

11429 Las pantallas ó monitores de computadoras deben orientarse para que no muestren datos sensibles por la exhibición hacia ventanas, pasillos públicos, puertas, etc.

11432 El movimiento de activos sensibles (Ej. medios magnéticos, reportes, etc.) á y desde la oficina debe ser controlado y registrado estrictamente.

11433 Cuando los activos sensibles (Ej. medios magnéticos, reportes, etc.), se transporten, se deben emplear las medidas de seguridad específicas (por ejemplo: cifrado o almacenamiento de datos en cajas fuertes).

Categoría del Riesgo: *Contingencia de la red de área local.*

Evaluación del Riesgo: Ó no existen acuerdos de contingencia para la red de área local ó los arreglos son débiles e ineficaces. Se debe dar atención con urgencia a esta área.

Contramedidas:

10950 Los requisitos mínimos de la red de área local, en términos de disponibilidad, funcionamiento y capacidad, deben ser definidos formalmente.

10951 Las instalaciones para la contingencia de la red de área local se deben probar por lo menos cada 12 meses.

Categoría del Riesgo: *Instalaciones Criptográficas en la LAN.*

Evaluación del Riesgo: Las instalaciones criptográficas para los datos que pasan por la red de área local son débiles y necesitan revisión. Esto es particularmente importante cuando los datos son confidenciales y cuando es esencial su integridad.

Contramedidas:

10952 Cuando los datos que pasan sobre la red de área local son de naturaleza confidencial, Se debe considerar la implementación de un mecanismo criptográfico.

10955 Cuando la integridad de datos es esencial, Se debe considerar la aplicación de una técnica de autentificación del mensaje (criptografía).

Categoría del Riesgo: *Control de Cambios.*

Evaluación del Riesgo: Los procedimientos del control de cambios son incompletos. El sistema tiene un número importante de vulnerabilidades en esta área. Se deben desarrollar procedimientos más a fondo y hacer que se cumplan estrictamente.

Contramedidas:

104002 Un procedimiento de control de cambios debe asegurar que la implementación de nuevo hardware y software, y los cambios al hardware y al software, han sido autorizados por escrito por la autoridad apropiada.

10403 Todos los cambios planeados deben tener un procedimiento de revocación acordado (debe ser activado en caso de problemas ó errores serios).

10410 Las mejoras de emergencia a los sistemas/componentes críticos deben ser siempre comprobadas/verificadas.

Categoría del Riesgo: *Controles y prácticas del cortafuegos.*

Evaluación del Riesgo: Algunos controles y prácticas desarrolladas de él cortafuegos están definidas e implementadas inadecuadamente. Fueron identificadas exposiciones potenciales las cuales requieren alguna atención.

Contramedidas:

70106 Cuando sea práctico, se debe utilizar una aproximación a la identidad doble en la cuál se utilizan dos tecnologías distintas en la aplicación de cortafuegos para asegurarse que una debilidad explotada en uno no compromete necesariamente al otro.

70115 Los registros de auditoria de él cortafuegos deben ser revisados y archivados de forma segura.

70115 Los registros de todas las tentativas de acceso exitosas y no exitosas en él cortafuegos deben ser registradas y revisadas.

Categoría del Riesgo: *Acceso y uso de Internet.*

Evaluación del Riesgo: Existen defectos claros con respecto a las prácticas de uso y acceso a Internet. Se requiere solucionar este problema.

Contramedidas:

60101 El Internet se debe utilizar solamente para actividades propias de la organización. La ruptura dé esto implica, una falta disciplinaria y todos los usuarios deben estar enterados del requerimientos.

60104 Los usuarios deben estar enterados de manera precisa del uso apropiado y eficaz del Internet.

Categoría del Riesgo: Prácticas de respaldos del Sistema y de datos.

Evaluación del Riesgo: Las prácticas de respaldo para las Pc’s son débiles. Esta área debe ser revisada tan pronto como sea posible.

Contramedidas:

10306 Si no es práctico realizar respaldos completos diariamente, por lo menos se deben hacer respaldos increméntales diarios, y se deben hacer por lo menos semanalmente los respaldos completos.

103007 Se recomienda que los respaldos completos del sistema se realicen por lo menos semanalmente.

10309 Si es aplicable, los respaldos se deben hacer de los datos de aplicaciones/usuarios así como de los datos/programas del sistema.

10311 Para los sistemas críticos, cuando se realice un respaldo, por lo menos se deben hacer dos copias.

Categoría del Riesgo: *Acceso a los datos sensibles.*

Evaluación del Riesgo: La protección de datos sensibles puede no ser suficiente. Un número de exposiciones son evidentes.

Contramedidas:

11101 Cuando se elimina un archivo altamente sensible, los datos dentro de ellos deben ser sobre escritos realmente (Ej. con ceros binarios).

11105 Para los datos altamente sensibles, el software de seguridad debe asegurarse de que los archivos protegidos puedan accederse solamente por los usuarios específicos o grupos de usuarios.

11106 Para los sistemas informáticos que contienen datos sensibles, se debe utilizar protección lógica y física (Ej. una llave de PC, un mecanismo de cerradura).

Categoría del Riesgo: *Control de Acceso y Autenticación.*

Evaluación del Riesgo: Los mecanismos de control de accesos y autenticación son básicos, produciendo una protección incompleta. Un acercamiento más comprensivo se debe considerar.

Contramedidas:

11201 Se recomienda que el acceso al sistema/red se. bloquee automáticamente por un período de tiempo fijo después de un número consecutivo de intentos de accesos fallidos al sistema.

11208 Cuando se cambia la contraseña de acceso, el sistema de seguridad debe forzar a ingresar la (vieja) contraseña existente para propósitos de validación.

11211 Se recomienda que por lo menos 13 generaciones de contraseña sean almacenadas en el archivo histórico del mecanismo de seguridad.

Categoría del Riesgo: Instalaciones Dial-in en la red de área local.

Evaluación del Riesgo: La administración y el control de las Instalaciones dial-in son débiles, exponiendo el sistema al nesgo. Se deben aplicar las recomendaciones rigurosamente.

Contramedida

10920 Se debe desarrollar una política/procedimiento para tener claramente definidos el uso de instalaciones dial-in. Está debe ser cumplida siempre estrictamente.

10922 Los números de teléfono Dial-in no deben ser iguales, o similares a los usados por la organización para otros propósitos, a menos que el acceso sea de dominio público.

10924 Los números de teléfono Dial-in deben ser cambiados si se sospecha de alguna falla de seguridad.

5.5 Trabajo futuro.

Lo que queda como trabajo futuro de este análisis es en primer lugar examinar los resultados obtenidos en este análisis de forma tal que se pueda dar principio a la estrategia de seguridad y entrar a la administración de riesgos que como se ha mencionado es la encargada de estudiar los riesgos, impactos y contra medidas o salvaguardas, tomar las decisiones de qué partes se deben tratar primero, dentro de este mismo espacio y para este estudio en especifico se deben tratar y estudiar las políticas resultantes de este trabajo, para poder definir que políticas se deben implantar y cuales no.

A la fecha en que se escribe estas líneas, ya se han hecho las recomendaciones necesaria y se ha empezado a trabajar con base en este documento en la forma en que los responsables han juzgado correcta.

Después de terminar el trabajo de administración de riesgos y que se determinó qué políticas se implantarán, seguirá la implantación de los controles y las políticas seleccionadas.

Al terminar la implantación de los controles y políticas de seguridad se le debe de dar seguimiento a este proceso y planear el inicio de un nuevo análisis de riesgos, siempre con la intención de poder implantar un sistema (ISMS) Sistema Administrativo de Seguridad de la Información obtenido con la correcta implantación de la norma BS 7799-2 e ISO/IEC 17799-1.

Bibliografía.

[1].ISO 17799: La nueva norma técnica global de seguridad.
http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_1261 .html

[21 En que consiste el 1S017799.
http://www.bulltek.com/Spanish_Site/ISO%209000%20INTRODUCClON/TL%209000%2OSpanish/lSO_1 7799_Spanish/iso_17799_spanish.html

(3] RFC 2196 - Site Security Handbook.
http://www.faqs.org/rfcs/rfc2196.html

[4] Políticas y Normatividad. Modulo 4 Diplomado de Seguridad Informática CEM-POLANCO UNAM. M en C. Leobardo Hernandez Audelo. Dr. Enrique Daltabuit Godas.

[5]NORMA IRAM-ISO/IEC 2000. Tecnología de la información.
Código de Práctica para la Administración de la Seguridad de la Información.

[6] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Criterios y sugerencias.
http://www.csi.rnap.es/csi/criterios/seguridad/criterios_seguridad.htm
http://www.csi.map.es/csi/criterios/seguridad/grafico6.htm

[7] Introducción a la Seguridad Informática. Modulo 1. Diplomado de Seguridad Informática CEM-POLANCO UNAM. M en C. Leobardo Hernandez Audelc. Dr. Enrique Daltabuit Godas.

[8] Metodología de Análisis y Gestión de riesgos de los Sistemas de Información. Guía de procedimientos. http://www.csi.map.es/csi/pg5m20.htm

[91 Pautas y recomendaciones para elaborar Políticas de Seguridad Informática. (PSI) por Jeimy J. CANO.
http://www.criptored.upm.es/guiateoria/gt_m142a.htm
http://www.ctv.es/USERS/mpq/estrado/estrado004.html#1

[10]Políticas y Procedimientos de Seguridad
http://www.seguridad.unam.mx/Tutoriales/Tutoriales/politicas/index.html

[11] Políticas de Seguridad. Juan Luis Chaves Sanabria.
Centro Nacional de Cálculo Científico (CeCaICULA)
Red de Datos de la Universidad de los Andes (RedULA)
Universidad de Los Andes - Mérida — Venezuela Octubre-Noviembre 2001.

[12]Las Políticas de Seguridad como Apoyo a la Falta de Legislación Informática.
M. Farias-Elinos, Ma. C. Mendoza-Díaz, & L. Gómez-Velazco. Techno-Legal Aspects of lnformation Society and New Economy: an Overview, Vol.1, pp. 185-191, Junio 2003, ISBN 84-607-8104-6
http://seguridad.internet2.ulsa.mx/publications/2003/002.pdf

[13] Site Security Handbook. Network Working Group. Request for Comments: 2196 B. Fraser Editor SEI/CMU September 1997. FYI: 8 Category: Informational
http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2196.html#sec-1.6

[14]MAGERIT Versión 1.0.
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
Guía de Aproximación a la Seguridad de los Sistemas de Información.
http://www.csi.map.es/csi/criterios/seguridad/criterios_seguridad.htm

[1 5]Risk Management.
http://www.projectmanagement.tas.gov.au/guidelines/pm5_6.htm

[16]Project Management Fact Sheet: Developing a Risk Management Plan
http://www.projectmanagement.tas.gov.au/guidelines/pm5_6.htm

[17]El método Delphi.
http://www.gtic.ssr.upm.eslencuestas/delphi.htm

[18] COBRA. Herramienta de análisis de riesgos.
http://www.securityauditor.ne/risk-analysis.htm
http://www.security-risk-analysis.com/

[19] Information Security Policies + Glossary ad Reference Manual Securing Information in the Digital Age. RUSecure - lnformation Security Policies

20] Pagina principal del proyecto nessus.
http://www.nessus.org/intro.html

INFORMATION TECHNOLOGY Baseline Protection Manual; capítulo 3.2;
http://www.bsi.bund.de/gshb/english/etc/inhalt.htm

ISOÍIEC TR 1333.5 - Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI- Partes 1, 2, y 3.

Guía de Seguridad Informática. http://www.sedisi.es/05_Estudios/guia01.htm

Análisis de riesgos.
http://es.tldp.org/ManuaIes-LuCAS/SEGUN IX/unixsec-2.1-html/node334.html

SEGURIDAD EN UNIX Y REDES Versión 2.1
Antonio Villalón Huerta Julio, 2002.

Guía de Seguridad Informática. SEDISI (Asociación Española de Empresas de Tecnologías de la información). http://www.sedisi.es/05_index.htm

Diario oficial de la nación fecha: 17 de mayo de 1999.

Titulo noveno. Revelación de secretos y acceso ilícito a sistemas y equipos de informática. http://www.textolandia.org.ar/txt/otros.html

Anexos.

ANEXO A1. Clasificación de controles específicos.

ANEXO A2. Controles y servicios de seguridad.

ANEXO A3. Relación entre amenazas y controles de mitigación.

ANEXO A4. Relación entre los servicios de seguridad y las amenazas.

ANEXO A5. Relación entre Vulnerabilidad, Amenaza y Activo.

ANEXO A6. Muestra de un cuestionario con respecto al 1S017799.

ANEXO A7. Muestra de un cuestionario con respecto al Consultor del Riesgo.

ANEXO AB. Políticas de seguridad para el instituto Mexicano del Petróleo.

Estos anexos se encuentran en el CD incluido en esta tesis.

ANEXO A2. CONTROLES Y SERVICIOS DE SEGURIDAD.							
SECCIÓN	**7799.2**	**Tipo de control.**					
		Confia-bilidad	Integ-ridad	Disponi-bilidad	Respon-sabilidad	Autenti-cidad	Confia-bilidad
3. CONTROLES ORGANISACIONALES Y ADMINISTRATIVOS.							
3.1 POLITICA DE LA SEGURIDAD DE LA INFORMACIÓN.	3.1	X	X	X	X		
3.2 INFRASTRUCTURA DE LA SEGURIDAD DE LA INFORMACIÓN.	4.1	X	X	X	X		
ASESORIA DE ESPECIALISTAS EN LA SEGURIDAD DE LA INFORMACIÓN.	4. 1.5						
COPERACION ENTRE ORGANIZACIONES.	4. 1.6						
REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN.	4. 1.7						
3.3 SECURIDAD DEL ACCESO A TERCEROS	4.2	X	X	X	X		X
3.4 OUTSOURCING.	4. 3	X	X	X	X		X
3.5 CÓMPUTO MOVIL.	9.8.1	X					
3.6 TELEWORKING	9.8.2						
3.7 CLASIFICACIÓN Y CONTROL DE ACTIVOS.	5.1	X	X	X	X		
CLASIFICACIÓN DE DIRECTRICES	5.2.1						
MANEJO Y ETIQUETADO DE INFORMACIÓN	5.2.2						
3.8 PRACTICAS DEL PERSONAL.							
3.8.1 DESCRIPCIONES DE TRABAJO.	6.1.1	X	X	X	X		
3.8.2 SEGREGACION DE RESPONSABILIDADES	8.1.4		X				
3.8.3 RECLUTAMIENTO.	6.1.2	X	X	X			
3.8.4 TERMINOS Y CONDICIONES DE EMPLEO.	6.1.3, 6.1.4	X	X	X	X		
3.8.5 MONITOREO DEL PERSONAL.	-	X	X	X	X		
3.8.6 TERMINACION Y CAMBIO DE TRABAJO.	-	X	X	X			
3.9 CONOCIMIENTO Y ENTRENAMIENTO DE LA SEGURIDAD.	6.2.1	X	X	X	X		
3.10 COMPLIMIENTO CON REQUIRIMINTOS LEGALES Y REGULADORES.	12.1						
IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE.	12.1.1	X	X	X			
DERECHOS DE PROPIEDAD INTELECTUAL.	12.1.2	X					
PROTEGER EXPEDIENTES DE LA ORGANISACIÓN.	12.1.3		X	X	X	X	
PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL.	12.1.4	X	X				
PREVENCIÓN DEL ABUSO DE LAS INSTALACIONES DE PROCESAMIENTO DE LA INFORMACIÓN.	12.1.5		X	X			
REGULACIÓN DE CONTROLES CRIPTOGRAFICOS.	12.1.6		X				
COLLECCIÓN DE EVIDENCIA.	12.1.7		X		X	X	
3.11 COMPLIMIENTO CON POLITICAS Y ESTANDARES DE SEGURIDAD.	12.2	X	X	X	X		
3.12 MANEJO DE INCIDENTES	6.3.1 a 6.3.4	X	X	X			
3.13 PROCESOS DISCIPLINARIOS.	6.3.5	X	X	X			

3.14 ADMINISTARCION DE LA CONTINUIDAD DEL NEGOCIO.	11.1			X			X
3.15 AUDITORIA DE SISTEMAS.							
3.15.1 AUDITORIAS DE SISTEMAS OPERACIONALES.	12.3.1		X				X
3.15.2 SYSTEM AUDIT TOOLS	12.3.2		X				X
4. CONTROLES FISICOS Y AMBIENTALES.							
4.1 AREAS SEGURAS.	7.1	X	X	X			
PERIMETRO DE SEGURIDAD FISICA.	7.1.1	X	X	X			
CONTROLES DE ACCESO FISICO.	7.1.2	X	X	X		X	
ASEGURAR OFICINAS, CUARTOS E INSTALACIONES.	7.1.3	X	X	X			
TRABAJAR EN AREAS SEGURAS.	7.1.4	X	X	X			
ÁREAS AISLADAS DE LA ENTREGA Y REPARTO.	7.1.5	X	X	X			
4.2 SEGURIDAD DEL EQUIPO	7.2						
LOCALIZACIÓN Y PROTECCIÓN DEL EQUIPO	7.2.1	X		X			X
SUMINISTROS DE ENERGIA.	7.2.2			X			X
SEGURIDAD DEL CABLEADO.	7.2.3	X	X	X			X
MANTENIMIENTO DEL EQUIPO.	4.5.2.4		X	X			X
SEGURIDAD DEL EQUIPO EXTERNO.	7.2.5	X	X	X			
SECURIDAD EN LA ELIMINACIÓN O REUTILIZACIÓN DEL EQUIPO.	7.2.6	X					
4.3 POLICA CLARA DE ESCRITORIO Y PANTALLA.	7.3.1						
4.4 EXTRACIÓN DE PROPIEDAES.	7.3.2						
5. CONTROLES OPERACIONALES							
5.1 DOCUMENTACIÓN	8.1.1		X		X		
5.2 CONFIGURACIÓN Y ADMINISTRACIÓN DE CAMBIOS.	8.1.2		X		X		X
5.3 MANEJO DE INCIDENTES.	8.1.3	X	X	X			
5.4 DESARROLLO DE SOFTWARE Y EVALUACIÓN DEL AMBIENTE.	8.1.5	X	X	X	X		X
5.5 INSTALACIONES OUTSOURCED.	8.1.6	X	X	X			
5.6 PLANEACIÓN DE SISTEMAS.	8.2.1		X	X			X
5.7 SISTEMAS Y PRUEBA DE ACEPTACIÓN.	8.2.2, 10.4.2		X	X			X
5.8 PROTECIÓN CONTRA CODIGO MALICIOSO.	8.3.1, 10.5.4	X	X	X			
5.9 RESPALDOS DE DATOS.	8.4.1		X	X			
5.10 CONEXIÓN	8.4.2, 8.4.3			X	X		
5.11 INTERCAMBIO DE SOFTWARE E INFORMACIÓN.	8.7.1	X	X	X	X		
5.12 SEGURIDAD DE LOS MEDIOS EN MOVIMIENTO.	8.7.2	X	X	X			X
5.13 SEGURIDAD DEL COMERCIO ELECTRONICO.	8.7.3	X	X			X	
5.13.1 INTERCAMBIO DE DATOS ELECTRÓNICOS (EDI).		X	X			X	
5.13.2 COMERCIO EN INTERNET.		X	X			X	
5.14 CORREO ELECTRONICO SEGURO.	8.7.4 4.6.7.4	X	X			X	
5.15 ELECTRONIC OFFICE SYSTEMS	8.7.5,	X		X			
5.16 PUBLICACIÓN ELECTRONICA.	8.7.6	X	X				
5.17 MEDIOS DE COMUNICACIÓN.	8.6	X	X	X			
6. CONTROLES TÉCNICOS.							
6.1 IDENTIFICACIÓN Y AUTENTICACIÓN.	9.3.1, 9.4.3 9.4.4,	X	X	X	X	X	

	9.5.3 9.5.4						
6.1.1 CONTRASEÑAS.	9.2.3, 9.3.1 9.4.3, 9.5.4	**X**	**X**		**X**	**X**	
6.1.2 COMPONENTES.	9.4.3	**X**	**X**		**X**	**X**	
6.1.3 DISPOSITIVOS BIOMETRICOS.	9.4.3	**X**	**X**		**X**	**X**	
6.2 ACCESOS LOGICOS.	9.1.1, 9.2.1 9.2.2, 9.2.3	**X**	**X**	**X**	**X**		
6.3 REVICIÓN DE DERECHOS DE ACCESO.	9.2.4	**X**	**X**	**X**	**X**		
6.4 HARDWARE DE USUARIO DESATENDIDO.	9.3.2, 9.5.7	**X**	**X**	**X**			
6.5 ADMINISTRACIÓN DE RED.	9.5.1, 9.4.1						
6.5.1 PROCEDIMIENTO OPERACIONALES.	9.4.1, 9.4.5	**X**	**X**	**X**			
6.5.2 RUTAS DE ACCESO DE USUARIO PREDEFINIDAS.	9.4.2	**X**	**X**				
6.5.3 CONTROLES DE ACCESO TELEFONICO.	9.4.3		**X**			**X**	
6.5.4 PALNEACIÓN DE RED.	8.5.1			**X**			**X**
6.5.5 CONFIGURACIÓN DE RED.	8.5.1			**X**			**X**
6.5.6 SEGREGACIÓN DE REDES.	9.4.6	X	X				
6.5.7 MONITOREO DE RED.	8.5.1				X		
6.5.8 DETECCIÓN DE INTRUSOS.	9.4.8		X				
6.5.9 POLITICAS DE CONEXIÓN A INTERNET	9.4.1, 9.4.7	X	X				
6.6 CONTROL DE ACCESO A SISTEMAS OPERATIVOS.							
6.6.1 IDENTIFICACIÓN AUTOMATICA DE TERMINALES Y ESTACIONES DE TRABAJO	9.5.1	X	X		X	X	
6.6.2 PRECEDIMIENTOS DE CONEXIÓN SEGURA.	9.5.2	X	X				
6.6.3 USO DE U5TILIDADES DEL SISTEMA.	9.5.5	X	X			X	
6.6.4 ALARMA DE COACCIÓN.	9.5.6	X	X	X			
6.6.5 RESTRICCIÓN DE TIEMPO.	9.5.8	X	X	X			
6.7.1 RESTRICCIÓN DE ACCESO A APLICACIÓN.	9.6.1	X	X				
6.7.2 AISLAMINETO DE APLICACIONE SENCIVLES.	9.6.2	X	X				
6.8 AUDITORIA DE GUELLAS Y BITACORAS.	9.7.1, 9.7.2 9.7.3	X	X		X		
7. DESARROLLO DE SISTEMAS Y CONTROLES DE MANTENIMIENTO.							
7.1 SEGURIDAD DE APLICACIÓNES.	10.2.1, 10.2.2, 10.2.3, 10.2.4	X	X				
7.2 CRIPTOGRAFIA.	10.3.1, 10.3.2 10.3.3, 10.3.4 10.3.5	X	X			X	
7.3 RESTRICCIONS PARA LA MODIFICACIÓN DE PAQUETES DE SOFTWARE.	10.5.3		X				X

ANEXO A3.	RELACIÓN ENTRE AMENAZAS Y CONTROLES DE MITIGACIÓN.										
SECCIÓN	**7799.2**	**AMENAZAS.**									
		fuego	**DDoS**	**Codigo malici-oso**	**Destruccion maliciosa de datos e insta-laciones**	**Suplan-tación**	**Robo y fraude**	**Intrusión al sitio web**	**Servicios de comunica-ción Fallido**	**Perdida de personal impor-tante**	**Error Operacional Del personal o Del usuario.**
3. CONTROLES ORGANISACIONALES Y ADMINISTRATIVOS.											
3.1 POLITICA DE LA SEGURIDAD DE LA INFORMACIÓN.	3.1	X	X	X	X	X	X	X	X	X	X
3.2 INFRASTRUCTURA DE LA SEGURIDAD DE LA INFORMACIÓN.	4.1			X							
ASESORIA DE ESPECIALISTAS EN LA SEGURIDAD DE LA INFORMACIÓN.	4. 1.5			X							
COPERACION ENTRE ORGANIZACIONES.	4. 1.6			X							
REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN.	4. 1.7	X	X	X	X	X	X	X	X	X	X
3.3 SECURIDAD DEL ACCESO A TERCEROS.	4.2		X		X		X				
3.4 OUTSOURCING.	4. 3							X		X	
3.5 CÓMPUTO MOVIL.	9.8.1						X				
3.6 TELEWORKING	9.8.2				X	X	X				
3.7 CLASIFICACIÓN Y CONTROL DE ACTIVOS.	5.1, 5.2	X		X	X		X		X		
CLASIFICACIÓN DE DIRECTRICES	5.2.1										
MANEJO Y ETIQUETADO DE INFORMACIÓN	5.2.2										
3.8 PRACTICAS DEL PERSONAL.											
3.8.1 DESCRIPCIONES DE TRABAJO.	6.1.1						X				
3.8.2 SEGREGACION DE RESPONSABILIDADES	8.1.4						X				
3.8.3 RECLUTAMIENTO.	6.1.2						X				
3.8.4 TERMINOS Y CONDICIONES DE EMPLEO.	6.1.3, 6.1.4						X				
3.8.5 MONITOREO DEL PERSONAL.	-	X		X	X		X			X	X

3.8.6 TERMINACION Y CAMBIO DE TRABAJO.	-						X				
3.9 CONOCIMIENTO Y ENTRENAMIENTO DE LA SEGURIDAD.	6.2.1	X	X	X	X	X	X	X	X	X	X
3.10 COMPLIMIENTO CON REQUIRIMINTOS LEGALES Y REGULADORES.	12.1										
IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE.	12.1.1	X									
DERECHOS DE PROPIEDAD INTELECTUAL.	12.1.2										
PROTEGER EXPEDIENTES DE LA ORGANISACIÓN.	12.1.3			X	X		X				
PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL.	12.1.4										
PREVENCIÓN DEL ABUSO DE LAS INSTALACIONES DE PROCESAMIENTO DE LA INFORMACIÓN.	12.1.5										
REGULACIÓN DE CONTROLES CRIPTOGRAFICOS.	12.1.6				X						
COLLECCIÓN DE EVIDENCIA.	12.1.7		X	X	X	X	X	X			
3.11 COMPLIMIENTO CON POLITICAS Y ESTANDARES DE SEGURIDAD.	12.2	X	X	X	X	X	X	X	X	X	X
3.12 MANEJO DE INCIDENTES	6.3.1, 6.3.4			X							X
3.13 PROCESOS DISCIPLINARIOS.	6.3.5			X	X		X				
3.14 ADMINISTARCION DE LA CONTINUIDAD DEL NEGOCIO.	11.1, 8.4.1	X	X	X	X		X		X		X
3.15 AUDITORIA DE SISTEMAS.											
3.15.1 AUDITORIAS DE SISTEMAS OPERACIONALES.	12.3.1				X		X				X
3.15.2 SYSTEM AUDIT TOOLS	12.3.2						X				X
4. CONTROLES FISICOS Y AMBIENTALES.											
4.1 AREAS SEGURAS.	7.1										
PERIMETRO DE SEGURIDAD FISICA.	7.1.1	X			X		X		X		
CONTROLES DE ACCESO FISICO.	7.1.2	X			X		X		X		
ASEGURAR OFICINAS, CUARTOS E INSTALACIONES.	7.1.3	X			X		X		X		

TRABAJAR EN AREAS SEGURAS.	7.1.4				X		X			X	
ÁREAS AISLADAS DE LA ENTREGA Y REPARTO.	7.1.5				X		X				
4.2 SEGURIDAD DEL EQUIPO	7.2										
LOCALIZACIÓN Y PROTECCIÓN DEL EQUIPO	7.2.1	X			X	X	X		X		
SUMINISTROS DE ENERGIA.	7.2.2	X			X						
SEGURIDAD DEL CABLEADO.	7.2.3				X				X		
MANTENIMIENTO DEL EQUIPO.	7.2.4	X									
SEGURIDAD DEL EQUIPO EXTERNO.	7.2.5				X		X				
SECURIDAD EN LA ELIMINACIÓN O REUTILIZACIÓN DEL EQUIPO.	7.2.6						X				
4.3 POLICA CLARA DE ESCRITORIO Y PANTALLA.	7.3.1				X	X	X				
4.4 EXTRACIÓN DE PROPIEDAES.	7.3.2						X				
5. CONTROLES OPERACIONALES											
5.1 DOCUMENTACIÓN	8.1.1				X					X	X
5.2 CONFIGURACIÓN Y ADMINISTRACIÓN DE CAMBIOS.	8.1.2			X	X						
5.3 MANEJO DE INCIDENTES.	8.1.3			X							X
5.4 DESARROLLO DE SOFTWARE Y EVALUACIÓN DEL AMBIENTE.	8.1.5				X						X
5.5 INSTALACIONES OUTSOURCED.	8.1.6										
5.6 PLANEACIÓN DE SISTEMAS.	8.2.1			X				X			
5.7 SISTEMAS Y PRUEBA DE ACEPTACIÓN.	8.2.2, 10.4.2			X							
5.8 PROTECIÓN CONTRA CODIGO MALICIOSO.	8.3.1, 10.5.4		X	X	X						
5.9 RESPALDOS DE DATOS.	8.4.1	X		X	X	X			X		X
5.10 CONEXIÓN	8.4.2, 8.4.3								X		X
5.11 INTERCAMBIO DE SOFTWARE E INFORMACIÓN.	8.7.1						X				
5.12 SEGURIDAD DE LOS MEDIOS EN MOVIMIENTO.	8.7.2			X	X		X				
5.13 SEGURIDAD DEL COMERCIO ELECTRONICO.	8.7.3										
5.13.1 INTERCAMBIO DE DATOS ELECTRÓNICOS (EDI).							X				

5.13.2 COMERCIO EN INTERNET.							X	X			
5.14 CORREO ELECTRONICO SEGURO.	8.7.4		X	X	X						X
5.15 ELECTRONIC OFFICE SYSTEMS	8.7.5, 8.7.7										X
5.16 PUBLICACIÓN ELECTRONICA.	8.7.6							X			
5.17 MEDIOS DE COMUNICACIÓN.	8.6				X		X				X
6. CONTROLES TÉCNICOS.											
6.1 IDENTIFICACIÓN Y AUTENTICACIÓN.	9.3.1, 9.4.3, 9.4.4, 9.5.3 9.5.4			X	X	X	X				
6.1.1 CONTRASEÑAS.	9.2.3, 9.3.1, 9.4.3, 9.5.4.			X		X		X			
6.1.2 COMPONENTES.	9.4.3					X		X			
6.1.3 DISPOSITIVOS BIOMETRICOS.	9.4.3					X		X			
6.2 ACCESOS LOGICOS.	9.1.1, 9.2.1, 9.2.2, 9.2.3			X	X	X					
6.3 REVICIÓN DE DERECHOS DE ACCESO.	9.2.4			X	X	X					
6.4 HARDWARE DE USUARIO DESATENDIDO.	9.3.2, 9.5.7			X	X	X	X				
6.5 ADMINISTRACIÓN DE RED.	9.5.1, 9.4.1,										
6.5.1 PROCEDIMIENTO OPERACIONALES.	9.4.1, 9.4.5					X			X	X	X
6.5.2 RUTAS DE ACCESO DE USUARIO PREDEFINIDAS.	9.4.2			X	X	X					
6.5.3 CONTROLES DE ACCESO TELEFONICO.	9.4.3		X	X	X	X		X			
6.5.4 PALNEACIÓN DE RED.	8.5.1							X		X	
6.5.5 CONFIGURACIÓN DE RED.	8.5.1							X		X	
6.5.6 SEGREGACIÓN DE REDES.	9.4.6		X	X	X	X		X	X		X
6.5.7 MONITOREO DE RED.	8.5.1		X	X	X	X		X	X		X
6.5.8 DETECCIÓN DE INTRUSOS.	9.4.8		X	X	X	X		X	X		
6.5.9 POLITICAS DE CONEXIÓN A INTERNET	9.4.1, 9.4.7		X	X	X	X					X
6.6 CONTROL DE ACCESO A SISTEMAS OPERATIVOS.											
6.6.1 IDENTIFICACIÓN AUTOMATICA DE TERMINALES Y ESTACIONES DE TRABAJO	9.5.1			X	X	X	X				

6.6.2 PRECEDIMIENTOS DE CONEXIÓN SEGURA.	9.5.2			X	X	X	X				
6.6.3 USO DE UTILIDADES DEL SISTEMA.	9.5.5			X	X	X	X				
6.6.4 ALARMA DE COACCIÓN.	9.5.6				X		X			X	
6.6.5 RESTRICCIÓN DE TIEMPO.	9.5.8			X	X	X	X				
6.7 CONTROL DE ACCESS A APLICACIONES.											
6.7.1 RESTRICCIÓN DE ACCESO A APLICACIÓN.	9.6.1			X	X	X	X				X
6.7.2 AISLAMINETO DE APLICACIONE SENCIVLES.	9.6.2			X	X	X	X				X
6.8 AUDITORIA DE GUELLAS Y BITACORAS.	9.7.1, 9.7.2 9.7.3			X	X	X	X				X
7. DESARROLLO DE SISTEMAS Y CONTROLES DE MANTENIMIENTO.											
7.1 SEGURIDAD DE APLICACIÓNES.	10.2.1, 10.2.2, 10.2.3, 10.2.4			X		X	X	X			X
7.2 CRIPTOGRAFIA.	10.3.1,10.3.2 10.3.3,10.3.4 10.3.5				X	X	X	X			
7.3 RESTRICCIONS PARA LA MODIFICACIÓN DE PAQUETES DE SOFTWARE.	10.5.3			X	X		X	X			

ANEXO A4. TABLA DE RELACIÓN ENTRE LOS SERVICIOS DE SEGURIDAD Y LAS AMENAZAS.

AMENAZAS	Respecto a la seguridad.					
	Confidencia-lidad	Integri-dad	Disponibi-lidad	Responsa-bilidad	Autentici-dad	Confiabi-lidad
Amenazas ambientales.						
Contaminación			X			
Terremoto			X			
Interferencia electrónica.			X			
Temperatura y humedad extremas.			X			
Falla del suministro de energía.			X			
Fuego.			X			
Inundación.			X			
Fluctuaciones de energía.			X			
Tormentas.			X			
Bichos.			X			
Amenazas deliberadas.						
Denegación de servicio.			X			
Escucha silenciosa.	X					
Fuego.			X			
Acción industrial.			X			
Código malicioso.	X	X	X			
Destrucción maliciosa de datos e instalaciones.		X	X	X		X
Suplantación.	X	X		X	X	
Repudiación.				X	X	
Sabotaje.		X	X			
Ingeniería social.	X	X	X	X	X	
Robo y fraude.	X		X	X	X	
Acceso no autorizado a los datos.	X	X		X	X	X
Acceso telefónico no autorizado.	X	X		X	X	X
Cambios de software no autorizados.	X	X	X	X		X
Uso de software pirata.			X	X		X
Intrusión al sitio web.	X	X	X		X	
Amenazas accidentales.						
Fuego en el edificio.			X			
Falla en los servicios de comunicaciones.			X			

Fallas de operaciones outsourced.	**X**	**X**	**X**			
Perdida o ausencia de personal importante.	**X**	**X**	**X**			**X**
Errores de ruteo/re-ruteo de mensajes.	**X**	**X**	**X**			
Errores operacionales del personal.		**X**	**X**			
Errores de software / Programación.	**X**	**X**	**X**			**X**
Fallas técnicas.		**X**	**X**			**X**
Errores de transmisión.		**X**	**X**			**X**

ANEXO A5. TABLA DE RELACIÓN ENTRE VULNERABILIDAD, AMENAZA Y ACTIVO.		
VULNERABILIDAD.	**AMENAZA.**	**TIPO DE ACTIVO.**
Disponibilidad de materiales inflamables tales como papel o cajas.	Fuego.	Instalaciones Hardware, Datos.
Respaldos de archivos y sistemas no disponibles.	Terremoto, Fuego, Inundación, Tormenta, Contaminación. Interferencia Electrónica. Temperatura y de la humedad extremos. Fluctuaciones de Energía. Los bichos. Falla de las operaciones outsourced, errores de transmisión, cambios de software no autorizados.	Instalaciones.
Interface de usuario complicada.	Errores de operación del personal o usuarios.	Datos
Acceso telefónico anuncio que conduce a la información la cual puede exponer la organización a un acceso telefónico no autorizado.	Acceso telefónico no autorizado.	Datos
Faltas en el proceso de administración de cambios.	Fallas técnicas.	Hardware
Cableado incorrecto o inadecuado.	Errores de transmisión.	Datos
Mantenimiento incorrecto o inadecuado de las instalaciones técnicas	Fallas técnicas.	Hardware
Control inadecuado de distribución de software.	Uso de Software pirata.	Software
Educación Inadecuada del personal en virus del software.	Código Malicioso	Datos
Políticas del firewall inadecuadas.	Intrusión al sitio Web. Acceso no autorizado a los datos Cambios en el software no autorizados. Destrucción maliciosa de datos e instalaciones. Robo y fraude.	Datos
Manejo inadecuado de incidentes.	Fallas de los servicios de comunicaciones. Errores de transmisión.	
Política de la seguridad de la información inadecuada.	Código malicioso.	Software
Supervisión inadecuada de condiciones ambientales	Temperatura y humedad extremas.	Instalaciones. Hardware.
Administración de red inadecuada.	Fallas de los servicios de comunicaciones.	Instalaciones.
Administración de red inadecuada. (resistencia de ruteo)	Denegación de servicio.	Instalaciones.
Divulgación y dirección inadecuada de los mal funcionamientos del software.	Cambios de software no autorizados	Software Datos
Segregación de deberes inadecuada entre los desarrolladores del software y el personal de operaciones.	Cambios de Software no autorizados.	Software Datos

Estándares Inadecuados de desarrollo de Software	Intrusión al sitio Web Site	Software
Supervisión inadecuada del personal de programación.	Cambios de software no autorizados.	Software Datos
Procedimientos inadecuados del ciclo de vida del desarrollo del sistema.	Errores de Software y Programación.	Software Datos
Entrenamiento inadecuado del usuario	Ruteo erróneo / re-rutear mensajes.	Datos
Derechos de acceso incorrectos	Sabotaje	Software Datos
Configuración/mantenimiento incorrecto de las características de seguridad de las aplicaciones.	Acceso no autorizado a los datos Destrucción maliciosa de datos. Robo y fraude.	Datos
Configuración/mantenimiento incorrecto de sistemas operativos.	Acceso no autorizado a los datos Cambios de software no autorizados. Destrucción maliciosa de datos Intrusión al sitio Web. Robo y fraude.	Software Datos
Configuración/mantenimiento incorrecto de los controles de seguridad.	Denegación de servicio. Acceso no autorizado a los datos. Cambios de software no autorizados. Destrucción maliciosa de datos. Intrusión al sitio Web. Robo y fraude.	Software Datos
Capacitación insuficiente en seguridad.	Errores de operación del personal y usuarios.	Datos
Carencia de un firewall.	Denegación de servicio. Accesos telefónico no autorizado. Acceso no autorizado a los datos. Cambios de software no autorizado. Destrucción maliciosa de datos. Intrusión al sitio web. Robo y fraude.	Datos Software
Carencia de un acuerdo industrial	Acción Industrial	Instalaciones Hardware Datos
Carencia de un inventario de conexiones telefónicas que provoca la inhabilidad de supervisar los accesos telefónicos.	Acceso telefónico no autorizado	Datos
Carencia de controles de aplicaciones para conducir los pagos fraudulentos que son hechos.	Robo y fraude.	Datos
Carencia de registros de auditoria para detectar accesos.	Acceso telefónico no autorizado.	Datos
Carencia del sistema automático de eliminación del fuego.	Fuego	Instalaciones.
Carencia de instalaciones de respaldos o procesos.	Fallas técnicas.	Instalaciones.
Carencia de respaldos.	Cambios de software no autorizados.	Software Datos
Carencia de controles de administración de cambios	Sabotaje	Software Datos.
Carencia de software de administración	Cambio de software no	Software

de cambios para implementar la administración de cambios.	autorizado.	
Carencia de la comunicación entre recursos humanos y el grupo de tecnologías de la información con respecto a la conducción de los empleados terminados para los empleados terminados que todavía tienen	Destrucción maliciosa de datos e instalaciones.	Instalaciones. Software Datos
Carencia de autenticación en la reconexión telefónica.	Acceso telefónico no autorizado.	Datos
Carencia de documentación operacional.	Errores del personal o usuarios.	Datos
Carencia de conducción efectiva en la administración de cambios del software para modificaciones no autorizadas de software que se podrían.	Robo y fraude.	Software Datos.
Carencia de control eficiente y eficaz en el cambio de configuración	Errores operacionales del personal y usuarios. Errores de Software/programación.	Software Datos
Carencia de protección ambiental.	Fallas técnicas.	Instalaciones. Hardware
Carencia de los dispositivos de detección del fuego.	Fuego	Instalaciones.
Carencia de mecanismo de identificación y autenticación.	Suplantación	Datos
Carencia de software detector de intrusos.	Acceso telefónico no autorizado. Intrusión al sitio Web Acceso no autorizado a los datos Cambios de software no autorizados. destrucción maliciosa de datos	Datos Software
Carencia de seguridad de acceso lógico.	Destrucción maliciosa de datos e instalaciones. Sabotaje. Robo y fraude.	Datos
Carencia de mantenimiento de equipo e instalaciones.	Contaminación	Instalaciones.
Carencia de la capacidad de red através de planeación y mantenimiento impropios.	Fallas técnicas.	Hardware
Carencia de seguridad física.	Fuego. Destrucción maliciosa de datos e instalaciones. Sabotaje. Robo y fraude. Acceso no autorizado a los datos	Instalaciones Hardware Datos
Carencia de seguridad física sobre los cuartos y hubs de comunicación de datos.	Escucha secreta.	Datos
Carencia de seguridad física sobre gabinetes de equipos de telecomunicaciones.	Acceso telefónico no autorizado	Datos
Carencia de planeación e implementación	Fallas de los servicios de comunicaciones	Datos
Carencia de políticas con respecto a las conexiones telefónicas, uso del módem, y uso del software.	Acceso telefónico no autorizado	Datos
Carencia de una política que requiera que	Ingeniería Social.	Software

la información sea retenida hasta que se investiga la identidad del solicitante.		Datos
Carencia de una política que restrinja al personal para usar el software con licencia	Uso de software pirata	Software
Carencia de una política que restrinja la disposición de la información del personal por teléfono.	Ingeniería Social	Software
Carencia de la prueba de recepción de un mensaje	Errores de ruteo/re-ruteo de mensajes.	Datos
Carencia de confirmación de enviar o de recibir un mensaje	Repudiación	Datos
Carencia de redundancia y respaldos.	Fallas de los servicios de comunicaciones.	Datos
Carencia de actualización regular de software antivirus.	Código malicioso	Software Datos
Carencia de auditoria de software	Use de software pirata	Software
Carencia de políticas y procedimientos de administración de cambios del software	Cambio no autorizado de software	Software Datos
Carencia de restricciones del tiempo en el acceso de usuarios	Acceso telefónico no autorizado.	Datos
Carencia de actualización de parches de seguridad en sistemas operativos	Intrusión al sitio Web	Software Datos
Carencia del uso de firmas digitales.	Repudiación	Datos
Carencia de autenticación de usuarios.	Acceso telefónico no autorizado	Software, Datos
Carencia de conocimiento del usuario sobre el software.	Errores operacionales del equipo y usuarios Fallas técnicas.	Datos Hardware
La localización está en un área susceptible a las condiciones ambientales tales como contaminación, interferencia electrónica, temperatura y humedad extrema, bichos.	Contaminación. Interferencia electrónica Temperatura y humedad extremas. Bichos.	Instalaciones.
La localización está en una área susceptible a desastres naturales.	Terremoto. Fuego. Inundación. Tormenta.	Instalaciones.
La localización está en una área susceptible a fallas de energía.	Fallas de energía	Instalaciones.
No hay software antivirus	Denegación de servicio Código malicioso	Software Datos.
No hay planes para la continuidad del negocio o procedimientos para recuperar información o activos de información.	Terremoto. Fuego. Inundación. Tormenta. Contaminación. Interferencia electrónica. Temperatura y humedad Extremas. Fallas de energía. Bichos. Fallas de operaciones outsourced. Acción industrial. Fallas técnicas. Errores de transmisión.	Instalaciones.
Ningún equipo de suministro de energía	Errores de energía	Hardware
Ningún equipo de suministro de energía continua.	Falla en el suministra de energía.	Hardware
El no contar con varias organizaciones de seguridad en línea tales como el CERT	Denegación de Servicio	Datos

conducirá a una debilidad conocida que no es corregida de una manera oportuna		
Transmisión de datos confidenciales sin encriptar.	Errores de ruteo/re-ruteo de mensajes. Acceso no autorizado a los datos	Datos
Obligaciones confusas en acuerdos del outsourcing.	Fallas de las operaciones outsourced.	Software Datos
Especificaciones confusas o incompletas	Errores de Software / Programación.	Software Datos
Copiado incontrolado de datos y/o de software	Robo y fraude	Datos, Documentos, Software
Uso y descarga incontrolada de software de Internet.	Código malicioso	Software
Comunicaciones no encriptadas	Escucha silenciosa	Datos
Tablas de contraseñas sin proteger	Suplantación	Datos
Copiado de software sin restricciones.	Use de software pirata	Software Datos
Uso de módem sin restricciones.	Acceso no autorizado a los datos.	Datos
Personal inexperto	Errores de software y Programación	Software Datos
El uso de Ethernet compartido significa que todo el tráfico es broadcast a cualquier máquina en un segmento local.	Escucha silenciosa	Datos

ANEXO A6. Muestra de un cuestionario con respecto al ISO17799.

Cuestionario del modulo: ASSETCLA - Clasificación y Control de Activos.

INTRODUCCION.

Los objetivos son mantener la protección adecuada de los activos corporativos y garantizar que los activos informáticos reciban un nivel adecuado de protección.

Sección 5 - Clasificación y Control de Activos.

Pregunta 1 – Se requiere la respuesta. Seleccione por favor solamente una respuesta.

¿Se mantienen los inventarios de los activos de hardware, software y datos?

No. Ir a la preguntar 4.
Sí.

Pregunta 2 – Se requiere la respuesta. Seleccione por favor solamente una respuesta.

¿Los activos tienen un dueño asignado?

No.
Sí.

Pregunta 3 - La respuesta es opcional, y más de una respuesta puede ser seleccionada.

¿Para cuáles de los siguientes no se mantiene un inventario?

Activos de información.
Activos de software.
Activos físicos.
Servicios.

Pregunta 4 – Se requiere la respuesta. Seleccione por favor solamente una respuesta.

¿Los activos de información tienen alguna clasificación de seguridad?

Sí.
No. Finalizar.

Pregunta 5 – Se requiere la respuesta. Seleccione por favor solamente una respuesta.

¿El esquema de clasificación permite el hecho de que la importancia de la información pueda cambiar (posiblemente de acuerdo con una política predeterminada)?

Sí.
No.
No es aplicable.

Pregunta 6 – Se requiere la respuesta. Seleccione por favor solamente una respuesta.

¿Se etiqueta la información clasificada?

Sí.
No. Ir a la pregunta 8.

Pregunta 7 - La respuesta es opcional, y más de una respuesta puede ser seleccionada.

¿Cuáles de los siguientes no son etiquetados con la clasificación apropiada?

Informes impresos.
Desplegados de pantalla.
Medios magnéticos.
Mensajes electrónicos.
Transferencias de archivos.

Pregunta 8 – Se requiere la respuesta. Seleccione por favor solamente una respuesta.

¿Están los procedimientos para el etiquetado de la información y dirección de acuerdo con el esquema de clasificación de la organización?

Sí.
No. Finalizar.

Pregunta 9 - La respuesta es opcional, y más de una respuesta puede ser seleccionada.

¿Cuál, si alguno, de los siguientes no es cubierto por los procedimientos del manejo de la información?

Copiado.
Almacenamiento.
Transmisión electrónica.
Transmisión hablada.
Destrucción.

ANEXO A7. Muestra de un cuestionario con respecto al Consultor del Riesgo.

A 01 evaluación del alto riesgo.

Reporte de la evaluación del riesgo.

Lista de preguntas y respuestas.

INTRODUCCIÓN.

Esta sección se produce para la inclusión como apéndice al informe de evaluación del riesgo. Enumera las preguntas y las respuestas obtenidas para cada módulo de la pregunta incluido en el cuestionario.

El informe también identifica la categoría del riesgo con la cual la pregunta se relaciona, junto con alguna cuenta atribuible a la respuesta.

Módulo De la Pregunta: AVAIL – Disponibilidad.

Pregunta 1.

¿Hay un plan formal y realizable de reanudación del negocio en el área?

Sí.
No.

Pregunta 2.

¿Que tan seguro esta usted de que el plan es adecuado para asegurar una recuperación y una continuación controladas del negocio dentro de los marcos de tiempo especificados como significantes/criticos?:

100% seguro.
Bastante seguro.
Seguro.
No muy seguro.
Preocupado.

Pregunta 3.

¿Cuándo fue probado el último plan de la continuidad del negocio?

Entre los ultimos 12 meses.
De 1 a 2 años.
De 2 a 3 años.
De 4 a 5 años.
Mas de 5 años atrás.

Pregunta 4.

¿Son los planes de contingencia razonables y apropiados para todos los componentes importantes?

Considere todos los componentes para los servicios de misión críticos. Éstos puden incluir las PC, software, módems, hardware, etc. Considere también si los planes existen para el reemplazo o la recuperación para los respaldos están dentro de un marco de tiempo aceptable.

Sí.

No.

Pregunta 5.

¿Que tan seguro esta usted de que los planes de contingencia y el plan de la continuidad del negocio permitirían la continuación y la recuperación eventual de la pérdida de un edificio importante (debido al fuego considerable, inundación, explosión, etc.) sin impacto serio o crítico en el negocio?

100% seguro.
Muy seguro.
Seguro.
No muy seguro.
Preocupado.

Pregunta 6.

¿Que tan seguro esta usted de que los planes de la contingencia y el plan de la continuidad del negocio permitirían la continuación y la recuperación eventual de la pérdida de personal importante (debido a un accidente serio, actividad industrial, etc.) sin impacto serio o crítico en el negocio?

100% seguro.
Muy seguro.
Seguro.
No muy seguro.
Preocupado.

Pregunta 7.

¿Ignorando los elementos de recuperación del plan de la continuidad del negocio, cual de los siguientes (si alguno), es el nivel de exposición critico? Considere el nivel critico si esta debajo notablemente o las vulnerabilidades incontroladas/atenuadas presentes podrían dar lugar a la indisponibilidad del servicio o a la pérdida de datos.

Fuego/inundación/explosión.
Hardware/mal funcionamiento del equipo.
Hardware/equipo/medios/otros.
Falla de energía.
Error del software.
Infección por virus de computadora.
Introducción de codigo malicioso.

Pregunta 8.

¿Ignorando los elementos de recuperación del plan de la continuidad del negocio, cual de los siguientes (si alguno), es el nivel de exposición critico? Considere el nivel critico si esta debajo notablemente o las vulnerabilidades incontroladas/atenuadas presentes podrían dar lugar a la indisponibilidad del servicio o a la pérdida de datos.

Hacking/sabotaje electrónico.
Perdida de la tercera parte del servicio.
Perdida de comunicación/servicios de red.
Error o sabotaje del operador.
Acción industrial por personal importante.
Otras amenazas.

Pregunta 9.

¿Existen las medidas específicas de respaldo y de recuperación para manejar la pérdida de datos críticos y el error serio del software de manera oportuna y apropiada?

Sí.
No.

Pregunta 10.

¿Son los controles de acceso/prácticas físicos apropiados para las áreas que pueden contener la información sensible o confidencial? Estas áreas pueden contener una variedad de entidades, tales como medios, nodos de red, computadoras, equipo ambiental, etc.

Ciertamente adecuado.
Generalmente bien.
Un motivo de preocupación.
Un problema importante.

Módulo De la Pregunta: BIA – Analisis del impacto del negocio.

Introducción.

Este módulo considera el carácter del negocio y del servicio de negocio. Examina las sensibilidades a los acontecimientos relacionados a la seguridad y se determina, si se requieren, otros pasos.

A través del ejercicio, las definiciones siguientes del impacto deben ser aplicadas:

Impacto SIGNIFICATIVO: Un impacto es ' significativo ' si da lugar a daño considerable al negocio.

Impacto CRÍTICO: Un impacto es ' crítico ' si pone la existencia del negocio en el riesgo.

En todos los casos, las preguntas se deben contestar con el peor panorama en mente (ej: el tiempo factible más extremo del impacto en el peor de los casos). También, las medidas de la contingencia y los controles existentes de la seguridad deben ser ignorados (la adecuación de éstos será considerada más adelante).

*** sobre la terminación de este módulo, las respuestas se debe determinar para establecer cuales otros módulos deben ser terminados. La dirección sobre esto se da DENTRO de este módulo de la pregunta.... considera las preguntas 6, 13 y 18. ***

Pregunta 1.

¿Cuál fue el ingreso total para esta función/servicio del negocio durante el ejercicio presupuestario pasado?

Menos de £ 100 mil.
De £100mil a £1millon.
De £1millon a £20millones.
Mas de £20millones.

Pregunta 2.

¿Cuál es el mayor rendimiento financiero probable total del valor por día?:

Menos de £5mil.

De £5mil a £50mil.
De £50mil a £500mil.
Mas de £500mil.

Pregunta 3.

¿Cuáles de los siguientes tipos de función se realizan directamente?:

Contabilidad financiera.
Negociar/repartir.
Nomina.
Administración información/soporte.
Investigación.
Fabricación.
Soporte de la infraestructura.
Venta al por menor.
Otros.

Pregunta 4.

¿Cuántos otros sistemas o unidades del negocio internos a esta empresa tienen una dependencia sobre ésta? Favor de especificar un numero para cada uno de los siguientes.

Poca dependencia.
Significante dependencia.
Total dependencia.

Pregunta 5.

¿Ha considerado cuidadosamente el alcance de este ejercicio en los términos de cual área/función/servicio se está evaluando? ¿Están los límites claros?

Sí.
No.

Pregunta 6.

Las preguntas siguientes pretenden establecer la sensibilidad del negocio a la ***no-disponibilidad*** del sistema o de los datos/información procesada.

*** Si el cuestionario se está terminando manualmente (en papel), la evaluación de la amenaza del módulo llamado AVAIL debe ser terminado si cualquiera de las primeras **dos** respuestas se selecciona para alguna de esas preguntas que identifican impacto **significativo**. Para las preguntas que identifican impacto **critico**, el módulo de evaluación de la amenaza AVAIL debe ser terminado si alguna de las primeras **tres** respuestas se seleccionan. ***

¿Esta usted listo para proceder?

Sí.
No.

Pregunta 7.

¿En el peor de los casos, que tan rápidamente podía la no-disponibilidad dar lugar a un impacto significativo en términos de los actuales/futuros ingresos y de otras pérdidas financieras directas?

2 horas.
24 horas.
7 días.
1 mes.
Nunca.

Pregunta 8.

¿En el peor de los casos, que tan rápidamente podía la no-disponibilidad dar lugar a un impacto critico en términos de los actuales/futuros ingresos y de otras pérdidas financieras directas?

2 horas.
24 horas.
7 días.
1 mes.
Nunca.

Pregunta 9.

¿En el peor de los casos, que tan rápidamente podía la no-disponibilidad tener un impacto significativo en términos de la confianza del cliente, del accionista, pública o departamental?

2 horas.
24 horas.
7 días.
1 mes.
Nunca.

Pregunta 10.

¿En el peor de los casos, que tan rápidamente podía la no-disponibilidad tener un impacto critico en términos de la confianza del cliente, del accionista, pública o departamental?

2 horas.
24 horas.
7 días.
1 mes.
Nunca.

Pregunta 11.

¿Que tan rápidamente podía la no-disponibilidad tener un impacto significativo en términos de obligaciones contractuales, reguladoras, o legales?

2 horas.
24 horas.
7 días.
1 mes.
Nunca.

Pregunta 12.

¿Que tan rápidamente podía la no-disponibilidad tener un impacto critico en términos de obligaciones contractuales, reguladoras, o legales?

2 horas.

24 horas.
7 días.
1 mes.
Nunca.

Pregunta 13.

Las preguntas siguientes pretenden establecer la sensibilidad del negocio a la pérdida de la ***confidencialidad*** de los datos/información procesada.

*** Si el cuestionario se está terminando manualmente (en papel), la evaluación de la amenaza del módulo llamado CONFID de debe ser terminado si una respuesta de significativo, de substancial o de critico se selecciona para cualquiera de las preguntas. ***

¿Esta usted listo para proceder?

Sí.
No.

Pregunta 14.

Si la confidencialidad de la información importante fue divulgada a unos o más competidores, cuál es el peor impacto que podría resultar:

Ninguna.
Moderado.
Significativo.
Considerable.
Critica.

Pregunta 15.

¿Si la confidencialidad de la información importante fue divulgada, cual podría ser el peor impacto en términos de los ingresos actuales/futuros y de otras pérdidas financieras directas?

Ninguna.
Moderado.
Significativo.
Considerable.
Critica.

Pregunta 16.

¿Si la confidencialidad de la información importante fue divulgada, cual podía ser el peor impacto en términos de la confianza del cliente, del accionista, pública o departamental?

Ninguna.
Moderado.
Significativo.
Considerable.
Critica.

Pregunta 17.

¿Si la confidencialidad de la información importante fue divulgada, habría implicaciones en términos de obligaciones contractuales, reguladoras, o legales?

Ninguna.
Moderado.
Significativo.
Considerable.
Critica.

Pregunta 18.

Las preguntas siguientes pretenden establecer la sensibilidad del negocio a la pérdida de la ***integridad*** de los datos/información procesada.

**** Si el cuestionario se está terminando manualmente (en papel), la evaluación de la amenaza del módulo llamado INTEG debe ser terminado si una respuesta de significativo, de substancial o de critico se selecciona para cualquiera de las preguntas. ****

¿Esta usted listo para proceder?

Sí.
No.

Pregunta 19.

¿Si los datos/información perdieron su integridad (por error, alteración deliberada no-autorizada, fraude, etc.), cual podría ser el peor impacto en términos de la pérdida financiera directa?

Ninguna.
Moderado.
Significativo.
Considerable.
Critica.

Pregunta 20.

¿Si los datos/información perdieron su integridad, cual podía ser el peor impacto en términos de la confianza del cliente, del accionista, pública o departamental?

Ninguna.
Moderado.
Significativo.
Considerable.
Critica.

Pregunta 21.

¿Si los datos/información perdieron su integridad, habría implicaciones en términos de obligaciones contractuales, reguladoras, o legales?

Ninguna.
Moderado.
Significativo.
Considerable.
Critica.

Pregunta 22.

¿Si los datos/información perdieron su integridad, cuál sería el peor impacto en términos de la interrupción de operaciones, de la inhabilidad para procesar datos del cliente, o de otras implicaciones adversas?

Ninguna.
Moderado.
Significativo.
Considerable.
Critica.

Pregunta 23.

El módulo del impacto del negocio se ha terminado. El paso siguiente es analizar las respuestas dadas para determinarse cuál, si algún, módulo de la amenaza necesitan ser terminados.

Si el cuestionario se ha terminado en papel, vea las preguntas 6, 13 y 18 como guia sobre la cual los módulos de la amenaza se han terminado.

¿Esta usted listo para proceder?

Sí.
No.

Módulo De la Pregunta: CONFID - confidencialidad.

Pregunta 1.

¿Que tan seguro esta usted de que no existe amenaza seria de terceros que ven información confidencial/sensible impresa no-autorizadas de salida?

100% seguro.
Muy seguro.
Seguro.
No muy seguro.
Preocupado.

Pregunta 2.

¿Existen los controles/practicas de acceso físico apropiados para el edificio?

Efectivamente adecuados.
Generalmente bien.
Una tema de inquietud.
Un problema importante.

Pregunta 3.

¿Existen los controles/practicas de acceso físico apropiado, para las áreas que mantienen la información sensible/confidencial?

Estas áreas pueden mantener esta información en una variedad de modos, por ejemplo, en documentos de papel, en medios de la computadora o el equipo (Ej. Los nodos de red) o la exhiben simplemente en un monitor.

Efectivamente adecuados.
Generalmente bien.

Una tema de inquietud.
Un problema importante.

Pregunta 4.

¿Existen los controles de acceso lógicos suficientes para proteger datos e información sensibles contra el análisis minucioso externo no-autorizado?

Sí... Ningunas debilidades evidentes.
Sí... Solamente debilidades de menor importancia.
No seguro.
Algunas preocupaciones.
Las debilidades importantes existen.

Pregunta 5.

¿Existen los controles de acceso lógicos apropiados y suficientes para proteger los datos/información sensible contra análisis minucioso interno no-autorizado?

Sí... Ningunas debilidades evidentes.
Sí... Solamente debilidades de menor importancia.
No seguro.
Algunas preocupaciones.
Las debilidades importantes existen.

Pregunta 6.

¿Son las prácticas con respecto al hardware, al equipo y a los medios adecuadas y apropiadas?

Efectivamente adecuados.
Generalmente bien.
Una tema de inquietud.
Un problema importante.

Pregunta 7.

Es la infraestructura de la seguridad y la cultura de la empresa:

Ejemplar.
Buena.
Razonable.
Posiblemente careciendo en una cierta área.
Pobre.

Pregunta 8.

¿Hay otras exposiciones evidentes?

Ningunas exposiciones importantes.
Algunos Preocupaciones.
Exposiciones importantes identificadas.

Pregunta 9.

¿Hay medidas/planes en lugar para atenuar o para manejar alguna violación de la confidencialidad?

Sí medidas comprensivas.
Sí planes del contorno.
Solamente ideas amplias.
No hay formales planes o medidas.

Módulo De la Pregunta: INTEG - Integridad.

Pregunta 1.

¿Que tan seguro esta usted de que no existe riesgo significativo de error serio, introducido durante la entrada de datos/información importante?

100% seguro.
Muy seguro.
Seguro.
No muy seguro.
Preocupado.

Pregunta 2.

Considere la situación con respecto a la manipulación intencional no-autorizada de la entrada de datos/información, por ambas partes internos y externos.

¿Que tan seguro esta usted de que no hay riesgo significativo de una violación seria durante la entrada de datos/información importante?

100% seguro.
Muy seguro.
Seguro.
No muy seguro.
Preocupado.

Pregunta 3.

¿Que tan seguro esta usted de que no hay riesgo significativo del error serio, introducido vía un error o mal funcionamiento del programa?

100% seguro.
Muy seguro.
Seguro.
No muy seguro.
Preocupado.

Pregunta 4.

¿Existen los controles apropiados en el área para prevenir la modificación no-autorizada del código fuente del programa?

Efectivamente adecuados.
Generalmente bien.
Una tema de inquietud.
Un problema importante.

Pregunta 5.

¿Existen los controles de acceso lógicos suficientes proteger los datos/información sensible contra el acceso externo no-autorizado?

Sí medidas comprensivas.
Sí planes del contorno.
Solamente ideas amplias.
No hay formales planes o medidas.

Pregunta 6.

¿Existen los controles de acceso lógicos apropiados y suficientes proteger los datos/información sensible contra el acceso interno no-autorizado?

Sí medidas comprensivas.
Sí planes del contorno.
Solamente ideas amplias.
No hay formales planes o medidas.

Pregunta 7.

¿Existen los controles sobre operaciones de computadora adecuados y apropiados?

Efectivamente adecuados.
Generalmente bien.
Una tema de inquietud.
Un problema importante.

Pregunta 8.

Es la infraestructura de la seguridad y la cultura de la empresa:

Ejemplar.
Buena.
Razonable.
Posiblemente careciendo en una cierta área.
Pobre.

Pregunta 9.

¿Hay otras exposiciones evidentes?

Ningunas exposiciones importantes.
Algunos Preocupaciones.
Exposiciones importantes identificadas.

Pregunta 10.

¿Hay medidas/planes en lugar para atenuar o para manejar alguna violación de la integridad?

Sí medidas comprensivas.
Sí planes del contorno.
Solamente ideas amplias.
No hay formales planes o medidas.

ANEXO A8. Políticas de seguridad para el Instituto Mexicano del Petróleo.

Estas políticas se obtuvieron en relación al resultado obtenido en el Análisis de Riesgos.

Soló políticas en inglés.

Planeación de la continuidad del negocio.

11.1.1

Policy 080101. Initiating the BCP Project.
"Management are required to initiate a Business Continuity Plan."

Policy 120303. Disaster Recovery Plan.
"Owners of the organisation's information systems must ensure that disaster recovery plans for their systems are developed, tested, and implemented."

Seguridad del personal.

6.1.1

Policy 090101. Preparing Terms and Conditions of Employment.
"The Terms and Conditions of Employment of this organisation are to include requirements for compliance with Information Security."

Policy 060107. Defending Against Hackers, Stealth-and Techno-Vandalism.
"Risks to the organisation's systems and information are to be minimised by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices."

Policy 090110. Employees' Responsibility to Protect Confidentiality of Data.
"All employees are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after contractual relations with the organisation."

Policy 090109. Establishing Ownership of Intellectual Property Rights.
"All employees and third party contractors are to sign a formal undertaking regarding the intellectual property rights of work undertaken during their terms of employment / contract respectively."

Policy 090108. Complying with Information Security Policy.
"All employees must comply with the Information Security Policies of the organisation. Any Information Security incidents resulting from non-compliance will result in immediate disciplinary action."

6.1.2

Policy 090102. Employing / Contracting New Staff.
"New employees' references must be verified, and the employees must undertake to abide by the organisation's Information Security policies."

Policy 090204. Checking Staff Security Clearance.
"All staff must have previous employment and other references carefully checked."

Policy 090203. Giving References on Staff.
"Only authorised personnel may give employee references."

Policy 030905. Speaking to the Media.
"Only authorised personnel may speak to the media (newspapers, television, radio, magazines etc.) about matters relating to the organisation."

Policy 090104. Using Non Disclosure Agreements (Staff and Third Party).
"Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is classified as Proprietary (or above)."

Policy 090303. Sharing Organisation Information with Other Employees.
"Confidential information should be shared only with other authorised persons."

Policy 130403. Breaching Confidentiality.
"Breaches of confidentiality must be reported to the Information Security Officer as soon as possible."

Policy 090601. Recommending Professional Advisors.
"The organisation does not encourage the recommending of professional advisors. References may however be given by authorised members of staff."

Policy 090316. Spreading Information through the Office 'Grape Vine'.
"All data and information not in the public domain, relating to the organisation's business and its employees, must remain confidential at all times."

Policy 090315. Gossiping and Disclosing Information.
"All data and information not in the public domain, relating to the organisation's business and its employees, must remain confidential at all times."

Policy 090314. Sharing Confidential Information with Family Members.
"All data and information not in the public domain, relating to the organisation's business and its employees, must remain confidential at all times."

Policy 090313. Responding to Telephone Enquiries.
"Telephone enquiries for sensitive or confidential information are initially to be referred to management. Only authorised persons may disclose information classified above Public, and then only to persons whose identity and validity to receive such information has been confirmed."

Policy 030906. Speaking to Customers.
"Information regarding the organisation's customers or other people dealing with the organisation is to be kept confidential at all times. The information should only released by authorised and trained persons."

6.2.1

Policy 050306. Training in New Systems.
"Training is to be provided to users and technical staff in the functionality and operations of all new systems."

Policy 060107. Defending Against Hackers, Stealth-and Techno-Vandalism.
"Risks to the organisation's systems and information are to be minimised by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices."

Policy 090107. Lending Money to Work Colleagues.
"Lending money to work colleagues is strongly discouraged."

Policy 090206. Sharing Personal Salary Information.
"Employees are discouraged from sharing personal salary details and other terms and conditions with other members of staff."

Policy 090308. Signing for the Delivery of Goods.
"Only authorised employees may sign for the receipt of goods. They are to ensure that, by signing for them, they are not considered to be verifying the quality or condition of the goods."

Policy 090310. Ordering Goods and Services.

"Only authorised persons may order goods on behalf of the organisation. These goods must be ordered in strict accordance with the organisation's purchasing policy."

Policy 110101. Delivering Awareness Programmes to Permanent Staff.
"Permanent staff are to be provided with Information Security awareness tools to enhance awareness and educate them regarding the range of threats and the appropriate safeguards."

Policy 110102. Third Party Contractor : Awareness Programmes.
"An appropriate summary of the Information Security Policies must be formally delivered to any such contractor, prior to any supply of services."

Policy 110103. Delivering Awareness Programmes to Temporary Staff.
"An appropriate summary of the Information Security Policies must be formally delivered to, and accepted by, all temporary staff, prior to their starting any work for the organisation."

Policy 110201. Information Security Training on New Systems.
"The organisation is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise Information Security."

Policy 110202. Information Security Officer : Training.
"Periodic training for the Information Security Officer is to be prioritised to educate and train in the latest threats and Information Security techniques."

Policy 110203. User : Information Security Training.
" Individual training in Information Security is mandatory, with any technical training being appropriate to the responsibilities of the user's job function. Where staff change jobs, their Information Security needs must be re-assessed and any new training provided as a priority."

Policy 110204. Technical Staff : Information Security Training.
"Training in Information Security threats and safeguards is mandatory, with the extent of technical training to reflect the job holder's individual responsibility for configuring and maintaining Information Security safeguards. Where IT staff change jobs, their Information Security needs must be re-assessed and any new training provided as a priority."

Policy 110205. Training New Recruits in Information Security.
"All new staff are to receive mandatory Information Security awareness training as part of induction."

Policy 130106. Being Alert for Fraudulent Activities.
"Employees are expected to remain vigilant for possible fraudulent activities."

Policy 130406. Detecting Electronic Eavesdropping and Espionage Activities.
"Where a risk assessment has identified an abnormal high risk from the threat of electronic eavesdropping and / or espionage activities, all employees will be alerted and reminded of the specific threats and the specific safeguards to be employed."

6.3.1

Policy 060110. Responding to Virus Incidents.
"The threat posed by the infiltration of a virus is high, as is the risk to the organisation's systems and data files. Formal procedures for responding to a virus incident are to be developed, tested and implemented. Virus Incident response must be regularly reviewed and tested."

Policy 070401. Recording Evidence of Incidents (Information Security).
"All employees are to be aware that evidence of Information Security incidents must be formally recorded and retained and passed to the appointed Information Security Officer."

Policy 130101. Reporting Information Security Incidents.
"All suspected Information Security incidents must be reported promptly to the appointed Information Security Officer."

Policy 130102. Reporting IS Incidents to Outside Authorities.
"Information Security incidents must be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This may only be done by authorised persons."

Policy 130103. Reporting Information Security Breaches.
"Any Information Security breaches must be reported without any delay to the appointed Information Security Officer to speed the identification of any damage caused, any restoration and repair and to facilitate the gathering of any associated evidence."

Policy 130105. Witnessing an Information Security Breach.
"Persons witnessing Information Security incidents or breaches should report them to the Information Security Officer without delay."

Policy 130203. Recording Information Security Breaches.
"Evidence relating to a suspected Information Security breach must be formerly recorded and processed."

6.3.2

Policy 130104. Notifying Information Security Weaknesses.
"All identified or suspected Information Security weaknesses are to be notified immediately to the Information Security Officer."

6.3.4

Policy 130301. Establishing Remedies to Information Security Breaches.
"A database of Information Security threats and 'remedies' should be created and maintained. The database should be studied regularly with the anecdotal evidence used to help reduce the risk and frequency of Information Security incidents in the organisation."

6.3.5

Policy 090101. Preparing Terms and Conditions of Employment.
"The Terms and Conditions of Employment of this organisation are to include requirements for compliance with Information Security."

Policy 090108. Complying with Information Security Policy.
"All employees must comply with the Information Security Policies of the organisation. Any Information Security incidents resulting from non-compliance will result in immediate disciplinary action."

Policy 090301. Using the Internet in an Acceptable Way.
"Employees may not use the organisation's systems to access or download material from the Internet which is inappropriate, offensive, illegal, or which jeopardises security. All Internet use must be for business related purposes."

Policy 090302. Keeping Passwords / PIN Numbers Confidential.
"All personnel must treat passwords as private and highly confidential. Non-compliance with this policy could result in disciplinary action."

Cumplimiento.

12.1.1

Policy 070101. Being Aware of Legal Obligations.
"Persons responsible for Human Resources Management are to ensure that all employees are fully aware of their legal responsibilities with respect to their use of computer based information systems and data. Such responsibilities are to be included within key staff documentation such as Terms and Conditions of Employment and the Organisation Code of Conduct."

Policy 070301. Safeguarding against Libel and Slander.
"Employees are prohibited from writing derogatory remarks about other persons or organisations."

Policy 070404. Recording Telephone Conversations.
"All parties are to be notified in advance whenever conversations are being recorded."

12.1.2

Policy 040104. Using Licensed Software.
"To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all End User Licence Agreements are to be strictly adhered to."

Policy 070103. Complying with General Copyright Legislation.
"Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Copyright, Designs and Patents Act legislation (or its equivalent), in so far as these requirements impact on their duties."

Policy 070104. Complying with Database Copyright Legislation.
"Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Copyright and Rights in Databases Regulations legislation (or its equivalent), in so far as these requirements impact on their duties."

Policy 070105. Complying with Copyright and Software Licensing Legislation.
"Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Software Copyright and Licensing legislation, in so far as these requirements impact on their duties."

Policy 070302. Using Copyrighted Information from the Internet.
"Information from the Internet or other electronic sources may not be used without authorisation from the owner of the copyright."

Policy 070303. Sending Copyrighted Information Electronically.
"Information from the Internet or other electronic sources may not be retransmitted without permission from the owner of the copyright."

Policy 070304. Using Text directly from Reports, Books or Documents.
"Text from reports, books or documents may not be reproduced or reused without permission from the copyright owner."

Policy 070402. Renewing Domain Name Licences – Web Sites.
"Registered domain names, whether or not actually used for the organisation's Web sites, are to be protected and secured in a similar manner to any other valuable asset of the organisation."

Policy 090109. Establishing Ownership of Intellectual Property Rights.
"All employees and third party contractors are to sign a formal undertaking regarding the intellectual property rights of work undertaken during their terms of employment / contract respectively."

12.1.3

Policy 030305. Retaining or Deleting Electronic Mail.
"Data retention periods for e-mail must be established to meet legal and business requirements and must be adhered to by all staff."

Policy 030502. Managing Data Storage.
"Day-to-day data storage must ensure that current data is readily available to authorised users and that archives are both created and accessible in case of need."

Policy 030503. Managing Databases.
"The integrity and stability of the organisation's databases must be maintained at all times."

Policy 030508. Archiving Documents.
"The archiving of documents must take place with due consideration for legal, regulatory and business issues with liaison between technical and business staff."

Policy 030509. Information Retention Policy.
"The information created and stored by the organisation's information systems must be retained for a minimum period that meets both legal and business requirements."

Policy 070201. Managing Media Storage and Record Retention.
"The organisation will maintain a suitable archiving and record retention procedure."

Policy 070403. Insuring Risks.
"A re-assessment of the threats and risks involved relating to the organisation's business activities must take place periodically to ensure that the organisation is adequately insured at all times."

12.1.4

Policy 030517. Updating Customer Information.
"Customer information may only be updated by authorised personnel. Customer data is to be safeguarded using a combination of technical access controls and robust procedures, with all changes supported by journals and internal audit controls."

Policy 030802. Sharing Information.
"Persons responsible for Human Resources Management are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organisation and to external parties."

Policy 030804. Maintaining Customer Information Confidentiality.
"Information relating to the clients and third party contacts of the organisation is confidential, and must be protected and safeguarded from unauthorised access and disclosure."

Policy 030805. Handling of Customer Credit Card Details.
"Customer credit card details entrusted to the organisation must be afforded a combination of security measures (technology and procedural) which, in combination, prevent all recognised possibilities of the card details being accessed, stolen, modified or an any other way divulged to unauthorised persons."

Policy 030906. Speaking to Customers.
"Information regarding the organisation's customers or other people dealing with the organisation is to be kept confidential at all times. The information should only released by authorised and trained persons."

Policy 030912. Checking Customer Credit Limits.
"Credit may only be advanced to customers once credit limits have been properly approved, in accordance with the organisation's usual financial credit control procedures."

Policy 070102. Complying with the Data Protection Act or Equivalent.
"The organisation intends to fully comply with the requirements of Data Protection legislation in so far as it directly affects the organisation's activities."

Policy 090110. Employees' Responsibility to Protect Confidentiality of Data.
"All employees are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after contractual relations with the organisation."

Policy 090201. Respecting Privacy in the Workplace.
"Notwithstanding the organisation's respect for employee's privacy in the workplace, it reserves the right to have access to all information created and stored on the organisation's systems."

Policy 090202. Handling Confidential Employee Information.
"All employee data is to be treated as strictly confidential and made available to only properly authorised persons."

Policy 090203. Giving References on Staff.
"Only authorised personnel may give employee references."

Policy 090205. Sharing Employee Information with Other Employees.
"Employee data may only be released to persons specifically authorised to receive this information."

Policy 090402. Taking Official Notes of Employee Meetings.
"Employee meeting and interview records must be formally recorded, with the contents classified as Highly Confidential and made available only to authorised persons."

12.1.5

Policy 030904. Using Photocopier for Personal Use.
"The use of photocopiers or duplicators for personal use is discouraged. In exceptions, specific permission may be given by the employee's immediate supervisor or manager."

Policy 070106. Legal Safeguards against Computer Misuse.
"Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Computer Misuse legislation (or its equivalent), in so far as these requirements impact on their duties."

Policy 070301. Safeguarding against Libel and Slander.
"Employees are prohibited from writing derogatory remarks about other persons or organisations."

Policy 090301. Using the Internet in an Acceptable Way.
"Employees may not use the organisation's systems to access or download material from the Internet which is inappropriate, offensive, illegal, or which jeopardises security. All Internet use must be for business related purposes."

Policy 090302. Keeping Passwords / PIN Numbers Confidential.
"All personnel must treat passwords as private and highly confidential. Non-compliance with this policy could result in disciplinary action."

Policy 090304. Using E-Mail and Postal Mail Facilities for Personal Reasons.
"The use of e-mail for personal use is discouraged, and should be kept to a minimum. Postal mail may be used for business purposes only."

Policy 090305. Using Telephone Systems for Personal Reasons.
"Personal calls on the telephone systems are to be minimised and limited to urgent or emergency use only."

Policy 090306. Using the Organisation’s Mobile Phones for Personal Use.
"The use of the organisation's mobile phones will to be monitored for inappropriate call patterns, unexpected costs, and excessive personal use."

Policy 090317. Playing Games on Office Computers.
"The playing of games on office PCs or laptops is prohibited."

Policy 090318. Using Office Computers for Personal Use.
"Using the organisation's computers for personal / private business is strongly discouraged."

12.1.6

Policy 030801. Using Encryption Techniques.
"Where appropriate, sensitive or confidential information or data should always be transmitted in encrypted form. Prior to transmission, consideration must always be given to the procedures to be used between the sending and recipient parties and any possible legal issues from using encryption techniques."

12.1.7

Policy 060103. Collecting Evidence for Cyber Crime Prosecution.
"Perpetrators of cyber crime will be prosecuted by the organisation to the full extent of the law. Suitable procedures are to be developed to ensure the appropriate collection and protection of evidence."

Policy 070401. Recording Evidence of Incidents (Information Security).
"All employees are to be aware that evidence of Information Security incidents must be formally recorded and retained and passed to the appointed Information Security Officer."

Policy 130202. Collecting Evidence of an Information Security Breach.
"Evidence relating to an Information Security breach must be properly collected and forwarded to the Information Security Officer."

Policy 060103. Collecting Evidence for Cyber Crime Prosecution.
"Perpetrators of cyber crime will be prosecuted by the organisation to the full extent of the law. Suitable procedures are to be developed to ensure the appropriate collection and protection of evidence."

Policy 070401. Recording Evidence of Incidents (Information Security).
"All employees are to be aware that evidence of Information Security incidents must be formally recorded and retained and passed to the appointed Information Security Officer."

Policy 130202. Collecting Evidence of an Information Security Breach.
"Evidence relating to an Information Security breach must be properly collected and forwarded to the Information Security Officer."

12.2.1

Policy 070202. Complying with Information Security Policy.
"All employees are required to fully comply with the organisation's Information Security policies. The monitoring of such compliance is the responsibility of management."

Policy 090108. Complying with Information Security Policy.
"All employees must comply with the Information Security Policies of the organisation. Any Information Security incidents resulting from non-compliance will result in immediate disciplinary action."

12.3.1

Policy 030211. Monitoring Operational Audit Logs.
"Operational audit logs are to be reviewed regularly by trained staff and discrepancies reported to the owner of the information system."

Policy 130401. Ensuring the Integrity of IS Incident Investigations.
"The use of information systems must be monitored regularly with all unexpected events recorded and investigated. Such systems must also be periodically audited with the combined results and history strengthening the integrity of any subsequent investigations."

12.3.2

Policy 130401. Ensuring the Integrity of IS Incident Investigations.
"The use of information systems must be monitored regularly with all unexpected events recorded and investigated. Such systems must also be periodically audited with the combined results and history strengthening the integrity of any subsequent investigations."

Clasificación y control de activos.

5.1.1

Policy 010601. Managing and Using Hardware Documentation**.**
“Hardware documentation must be kept up-to-date and readily available to the staff who are authorised to support or maintain systems.”

Policy 010602. Maintaining a Hardware Inventory or Register.
“A formal Hardware Inventory of all equipment is to be maintained and kept up to date at all times.”

Policy 050401. Documenting New and Enhanced Systems.
“All new and enhanced systems must be fully supported at all times by comprehensive and up to date documentation. New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available.”

Policy 140106. Accepting Ownership for Classified Information.
"All information, data and documents are to be the responsibility of a designated information owner or custodian."

5.2.1

Policy 030519. Using Headers and Footers.
"A document's security classification level and ownership should be stated within the header and footer space on each page of all documents."

Policy 030801. Using Encryption Techniques.
"*Where appropriate, sensitive or confidential information or data should always be transmitted in encrypted form. Prior to transmission, consideration must always be given to the procedures to be used between the sending and recipient parties and any possible legal issues from using encryption techniques."*

Policy 030802. Sharing Information.
"Persons responsible for Human Resources Management are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organisation and to external parties."

Policy 030808. Dealing with Sensitive Financial Information.
"Sensitive financial information is to be classified as Highly Confidential and must be afforded security measures (technology and procedural) which, in combination, safeguard such information from authorised access and disclosure."

Policy 140101. Defining Information.
"The organisation must record, maintain and update a data base of its information assets."

5.2.2

Policy 030513. Updating Draft Reports.
"Draft reports should only be updated with the authority of the designated owner of the report."

Policy 030518. Using Meaningful File Names.
"The naming of the organisation's data files must be meaningful and capable of being recognised by its intended users."

Policy 030519. Using Headers and Footers.
"A document's security classification level and ownership should be stated within the header and footer space on each page of all documents."

Policy 030522. Saving Data / Information by Individual Users.
"All users of information systems whose job function requires them to create or amend data files, must save their work on the system regularly in accordance with best practice, to prevent corruption or loss through system or power malfunction."

Policy 030710. Transporting Sensitive Documents.
"The designated owners of documents which contain sensitive information are responsible for ensuring that the measures taken to protect their confidentiality, integrity and availability, during and after transportation / transmission, are adequate and appropriate."

Policy 140102. Labelling Classified Information.
"All information, data and documents are to be clearly labelled so that all users are aware of the ownership and classification of the information."

Policy 140104. Isolating Top Secret Information.
"All information, data or documents classified as highly sensitive (Top Secret) must be stored in a separate secure area."

Seguridad de la Organización.

4.1.2

Policy 110104. Drafting Top Management Security Communications to Staff.
"The senior management of the organisation will lead by example by ensuring that Information Security is given a high priority in all current and future business activities and initiatives."

Policy 110105. Providing Regular Information Updates to Staff.
"The organisation is committed to providing regular and relevant Information Security awareness communications to all staff by various means, such as electronic updates, briefings, newsletters, etc."

Policy 030201. Appointing System Administrators.
"The organisation's systems are to be managed by a suitably qualified systems administrator who is responsible for overseeing the day to day running and security of the systems."

Policy 030202. Administrating Systems.
"System Administrators must be fully trained and have adequate experience in the wide range of systems and platforms used by the organisation. In addition, they must be knowledgeable and conversant with the range of Information Security risks which need to be managed."

Policy 050203. Establishing Ownership for System Enhancements.
“All proposed system enhancements must be business driven and supported by an agreed Business Case. Ownership (and responsibility) for any such enhancements will intimately rest with the business owner of the system.”

Policy 060108. Handling Hoax Virus Warnings.
"Procedures to deal with hoax virus warnings are to be implemented and maintained."

Policy 090103. Contracting with External Suppliers / other Service Providers.
"All external suppliers who are contracted to supply services to the organisation must agree to follow the Information Security policies of the organisation. An appropriate summary of the Information Security Policies must be formally delivered to any such supplier, prior to any supply of services."

4.1.4

Policy 010101. Specifying Information Security Requirements for New Hardware.
"All purchases of new systems hardware or new components for existing systems must be made in accordance with Information Security and other organisation Policies, as well as technical standards. Such requests to purchase must be based upon a User Requirements Specification document and take account of longer term organisational business needs."

Policy 010102. Specifying Detailed Functional Needs for New Hardware.
“Except for minor purchases, hardware must be purchased through a structured evaluation process which must include the development of a detailed Request For Proposal (RFP) document. Information Security features and requirements must be identified within the RFP.”

Policy 010103. Installing New Hardware.
“All new hardware installations are to be planned formally and notified to all interested parties ahead of the proposed installation date. Information Security requirements for new installations are to be circulated for comment to all interested parties, well in advance of installation.”

Policy 010104. Testing Systems and Equipment.
“All equipment must be fully and comprehensively tested and formally accepted by users before being transferred to the live environment.”

Policy 040101. Specifying User Requirements for Software.
"All requests for new applications systems or software enhancements must be presented to senior management with a Business Case with the business requirements presented in a User Requirements Specification document."

Policy 040102. Selecting Business Software Packages.
“The organisation should generally avoid the selection of business critical software which, in the opinion of management, has not been adequately proven by the early adopters of the system. The selection process for all new business software must additionally incorporate the criteria upon which the selection will be made. Such criteria must receive the approval of senior management.”

Policy 040103. Selecting Office Software Packages.
“All office software packages must be compatible with the organisation’s preferred and approved computer operating system and platform.”

Policy 050204. Justifying New System Development.
“The development of bespoke software is only to be considered, if warranted by a strong Business Case and supported both by management and adequate resources over the projected life time of the resultant project.”

4.2.1

Policy 030204. Permitting Third Party Access.
"Third party access to corporate information is only permitted where the information in question has been ‘ring fenced’ and the risk of possible unauthorised access is considered to be negligible."

4.2.2

Policy 030903. Using External Disposal Firms.
"Any third party used for external disposal of the organisation's obsolete equipment and material must be able to demonstrate compliance with this organisation’s Information Security Policies and also, where appropriate, provide a Service Level Agreement which documents the performance expected and the remedies available in case of non compliance."

Policy 040205. Supporting Application Software.
“All application software must be provided with the appropriate level of technical support to ensure that the organisation’s business is not compromised by ensuring that any software problems are handled efficiently with their resolution available in an acceptable time.”

Policy 050501. Acquiring Vendor Developed Software.
“Vendor developed software must meet the User Requirements Specification and offer appropriate product support.”

Policy 090309. Signing for Work done by Third Parties.
"Only properly authorised persons may sign for work done by third parties."

Policy 090311. Verifying Financial Claims and Invoices.
"All claims for payment must be properly verified for correctness before payment is effected."

Policy 100104. Using External Service Providers for E-Commerce.
"Where third parties are involved in e-commerce systems and delivery channels, it is essential that they are able to meet the resilience and Information Security objectives of the organisation."

Policy 110102. Third Party Contractor : Awareness Programmes.
"An appropriate summary of the Information Security Policies must be formally delivered to any such contractor, prior to any supply of services."

Policy 130403. Breaching Confidentiality.
"Breaches of confidentiality must be reported to the Information Security Officer as soon as possible."

Sistemas de Control de Accesos.

9.1.1

Policy 020101. Managing Access Control Standards.
“Access control standards for information systems must be established by management and should incorporate the need to balance restrictions to prevent unauthorised access against the need to provide unhindered access to meet business needs.”

Policy 030301. Downloading Files and Information from the Internet.
“Great care must be taken when downloading information and files from the Internet to safeguard against both malicious code and also inappropriate material.”

Policy 030306. Setting up Intranet Access.
"Persons responsible for setting up Intranet access must ensure that any access restrictions pertaining to the data in source systems, are also applied to access from the organisation’s Intranet."

Policy 030307. Setting up Extranet Access.
"Persons responsible for setting up Extranet access must ensure that any access restrictions pertaining to the data in source systems, are also applied to access from the organisation’s Extranet".

Policy 030308. Setting up Internet Access.
"Persons responsible for setting up Internet access are to ensure that the organisation’s network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. Human Resources management must ensure that all personnel with Internet access (including e-mail) are aware of, and will comply with, an acceptable code of conduct in their usage of the Internet in addition to compliance with the organisation’s Information Security Policies."

Policy 030312. Using Internet for Work Purposes.
"Management is responsible for controlling user access to the Internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security incidents."

Policy 030317. Filtering Inappropriate Material from the Internet.
"The organisation will use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by staff. Reports of attempted access will be scrutinised by management on a regular basis."

Policy 030506. Setting up a New Folder / Directory.
"Data directories and structures should be established by the owner of the information system with users adhering to that structure. Access restrictions to such directories should be applied as necessary to restrict unauthorised access."

Policy 030507. Amending Directory Structures.
"Existing directory and folder structures may only be amended with the appropriate authorisation, usually from the owner of the information system concerned."

Policy 030513. Updating Draft Reports.
"Draft reports should only be updated with the authority of the designated owner of the report."

Policy 030514. Deleting Draft Reports.
"Draft version(s) of reports must be deleted or archived following production of a final version. A single version of the file should be retained for normal operational access."
Policy 030516. Sharing Data on Project Management Systems.
"Only authorised persons may access sensitive or confidential data on projects owned or managed by the organisation or its employees."

Policy 030809. Deleting Data Created / Owned by Others.
"Data is to be protected against unauthorised or accidental changes, and may only be deleted with the proper authority."

Policy 030810. Protecting Documents with Passwords.
"Sensitive / confidential electronic data and information should be secured, whenever possible, with access control applied to the directory on the (computer) system concerned. The sole use of passwords to secure individual documents is less effective, and hence discouraged, as passwords may be either forgotten or become revealed (over time) to unauthorised persons."

Policy 060104. Defending Against Premeditated Internal Attacks.
"In order to reduce the incidence and possibility of internal attacks, access control standards and data classification standards are to be periodically reviewed whilst maintained at all times."

Policy 100102. Securing E-Commerce Networks.
"e-commerce related Web site(s) and their associated systems are to be secured using a combination of technology to prevent and detect intrusion together with robust procedures using dual control, where manual interaction is required."

9.2.1

Policy 090501. Handling Staff Resignations.
"Upon notification of staff resignations, Human Resources management must consider with the appointed Information Security Officer whether the member of staff's continued system access rights constitutes an unacceptable risk to the organisation and, if so, revoke all access rights."

9.2.2

Policy 090501. Handling Staff Resignations.
"Upon notification of staff resignations, Human Resources management must consider with the appointed Information Security Officer whether the member of staff's continued system access rights constitutes an unacceptable risk to the organisation and, if so, revoke all access rights."

9.2.3

Policy 020106. Managing Passwords.
"The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. In particular, passwords shall not be shared with any other person for any reason."

9.2.4

Policy 020101. Managing Access Control Standards.
"Access control standards for information systems must be established by management and should incorporate the need to balance restrictions to prevent unauthorised access against the need to provide unhindered access to meet business needs."

Policy 020110. Giving Access to Files and Documents.
"Access to information and documents is to be carefully controlled, ensuring that only authorised personnel may have access to sensitive information."

Policy 090501. Handling Staff Resignations.
"Upon notification of staff resignations, Human Resources management must consider with the appointed Information Security Officer whether the member of staff's continued system access rights constitutes an unacceptable risk to the organisation and, if so, revoke all access rights."

Policy 090502. Completing Procedures for Staff Leaving Employment.
"Departing staff are to be treated sensitively, particularly with regard to the termination of their access privileges."
Policy 090503. Obligations of Staff Transferring to Competitors.
"System and information access rights of employees who are transferring to competitors must be terminated immediately."

Policy 020106. Managing Passwords.
“The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. In particular, passwords shall not be shared with any other person for any reason.”

9.5.2

Policy 020106. Managing Passwords.
“The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. In particular, passwords shall not be shared with any other person for any reason.”

9.5.4

Policy 020106. Managing Passwords.
“The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. In particular, passwords shall not be shared with any other person for any reason.”

9.5.8

Policy 020101. Managing Access Control Standards.
“Access control standards for information systems must be established by management and should incorporate the need to balance restrictions to prevent unauthorised access against the need to provide unhindered access to meet business needs.”

9.6.1

Policy 020108. Restricting Access.
“Access controls are to be set at an appropriate level which minimises information security risks yet also allows the organisation's business activities to be carried without undue hindrance.”

Policy 060104. Defending Against Premeditated Internal Attacks.
"In order to reduce the incidence and possibility of internal attacks, access control standards and data classification standards are to be periodically reviewed whilst maintained at all times."

9.6.2

Policy 020111. Managing Higher Risk System Access.
“Access controls for highly sensitive information or high risk systems are to be set in accordance with the value and classification of the information assets being protected.”

Policy 140104. Isolating Top Secret Information.
"All information, data or documents classified as highly sensitive (Top Secret) must be stored in a separate secure area."

9.7.1

Policy 030208. Monitoring Error Logs.
"Error logs must be properly reviewed and managed by qualified staff."

Policy 070401. Recording Evidence of Incidents (Information Security).
"All employees are to be aware that evidence of Information Security incidents must be formally recorded and retained and passed to the appointed Information Security Officer."

9.7.2

Policy 020109. Monitoring System Access and Use.
“Access is to be logged and monitored to identify potential misuse of systems or information.”

Policy 030208. Monitoring Error Logs.
"Error logs must be properly reviewed and managed by qualified staff."

Policy 060104. Defending Against Premeditated Internal Attacks.
"In order to reduce the incidence and possibility of internal attacks, access control standards and data classification standards are to be periodically reviewed whilst maintained at all times."
Policy 070401. Recording Evidence of Incidents (Information Security).
"All employees are to be aware that evidence of Information Security incidents must be formally recorded and retained and passed to the appointed Information Security Officer."

Policy 100102. Securing E-Commerce Networks.
"e-commerce related Web site(s) and their associated systems are to be secured using a combination of technology to prevent and detect intrusion together with robust procedures using dual control, where manual interaction is required."

Policy 130401. Ensuring the Integrity of IS Incident Investigations.
"The use of information systems must be monitored regularly with all unexpected events recorded and investigated. Such systems must also be periodically audited with the combined results and history strengthening the integrity of any subsequent investigations."

9.8.1

Policy 010402. Issuing Laptop / Portable Computers to Personnel.
“Line management must authorise the issue of portable computers. Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices.”

Policy 010403. Using Laptop/Portable Computers.
“Persons who are issued with portable computers and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimise the risks.”

Policy 010407. Using Business Centre Facilities.
“Personnel using business centres to work on the organisation’s business are responsible for ensuring the security and subsequent removal and deletion of any information entered into the business centre's systems.”

Policy 010408. Day to Day Use of Laptop / Portable Computers.
“Laptop computers are to be issued to, and used only by, authorised employees and only for the purpose for which they are issued. The information stored on the laptop is to be suitably protected at all times.”

Policy 030602. Backing up Data on Portable Computers.
"Information and data stored on Laptop or portable computers must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis."

Policy 030911. Travelling on Business.
"Employees travelling on business are responsible for the security of information in their custody."

9.8.2

Policy 010404. Working from Home or Other Off-Site Location (Tele-working).
“Off-site computer usage, whether at home or at other locations, may only be used with the authorisation of line management. Usage is restricted to business purposes, and users must be aware of and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures.”

Administración de Operaciones y Equipo de Cómputo.

8.1.1

Policy 030209. Scheduling Systems Operations.
"Systems Operations schedules are to be formally planned, authorised and documented."

8.1.2

Policy 030210. Scheduling Changes to Routine Systems Operations.
"Changes to routine systems operations are to be fully tested and approved before being implemented."

8.1.3

Policy 060106. Safeguarding Against Malicious Denial of Service Attack.
"Contingency plans for a denial of service attack are to be maintained and periodically tested to ensure adequacy."

Policy 060110. Responding to Virus Incidents.
"The threat posed by the infiltration of a virus is high, as is the risk to the organisation's systems and data files. Formal procedures for responding to a virus incident are to be developed, tested and implemented. Virus Incident response must be regularly reviewed and tested."

Policy 130204. Responding to Information Security Incidents.
"The Information Security Officer must respond rapidly but calmly to all Information Security incidents, liaising and coordinating with colleagues to both gather information and offer advice."

Policy 130402. Analysing IS Incidents Resulting from System Failures.
"Information Security incidents arising from system failures are to be investigated by competent technicians."

Policy 130404. Establishing Dual Control / Segregation of Duties.
" During the investigation of Information Security incidents, dual control and the segregation of duties are to be included in procedures to strengthen the integrity of information and data."

Policy 130405. Using Information Security Incident Check Lists.
"Staff shall be supported by management in any reasonable request for assistance together with practical tools, such as security incident checklists, etc., in order to respond effectively to an Information Security incident."

Policy 130407. Monitoring Confidentiality of nformation Security Incidents.
"Information relating to Information Security incidents may only be released by authorised persons."

8.1.4

Policy 030901. Using Dual Input Controls.
"The decision whether dual control is required for data entry is to be made by the information system owner. Where so required, secure data handling procedures including dual input are to be strictly adhered to."

Policy 030907. Need for Dual Control / Segregation of Duties.
"The techniques of dual control and segregation of duties are to be employed to enhance the control over procedures wherever both the risk from, and consequential impact of, a related Information Security incident would likely result in financial or other material damage to the organisation."

Policy 050206. Separating Systems Development and Operations.
"Management must ensure that proper segregation of duties applies to all areas dealing with systems development, systems operations, or systems administration."

Policy 130404. Establishing Dual Control / Segregation of Duties.
" During the investigation of Information Security incidents, dual control and the segregation of duties are to be included in procedures to strengthen the integrity of information and data."

8.1.5

Policy 050201. Software Development.
"Software developed for or by the organisation must always follow a formalised development process which itself is managed under the project in question. The integrity of the organisation's operational software code must be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures."

Policy 050206. Separating Systems Development and Operations.
"Management must ensure that proper segregation of duties applies to all areas dealing with systems development, systems operations, or systems administration."

8.2.1

Policy 050304. Capacity Planning and Testing of New Systems.
“New systems must be tested for capacity, peak loading and stress testing. They must demonstrate a level of performance and resilience which meets or exceeds the technical and business needs and requirements of the organisation.”

8.3.1

Policy 030104. Defending your Network Information from Malicious Attack.
"System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion."

Policy 030301. Downloading Files and Information from the Internet.
“Great care must be taken when downloading information and files from the Internet to safeguard against both malicious code and also inappropriate material.”

Policy 030304. Receiving Electronic Mail (E-mail).
"Incoming e-mail must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code."

Policy 030318. Certainty of File Origin.
"Computer files received from unknown senders are to be deleted without being opened."

Policy 030505. Receiving Information on Disks.
"The use of removable media disks e.g. disks and CD-ROMs is not permitted except where specifically authorised."

Policy 030902. Loading Personal Screen Savers.
"Employees are not permitted to load non-approved screen savers onto the organisation's PCs, laptops and workstations."

Policy 060108. Handling Hoax Virus Warnings.
"Procedures to deal with hoax virus warnings are to be implemented and maintained."

Policy 060109. Defending Against Virus Attacks.
"Without exception, Anti Virus software is to be deployed across all PCs with regular virus definition updates and scanning across both servers, PCs and laptop computers."

Policy 060110. Responding to Virus Incidents.
"The threat posed by the infiltration of a virus is high, as is the risk to the organisation’s systems and data files. Formal procedures for responding to a virus incident are to be developed, tested and implemented. Virus Incident response must be regularly reviewed and tested."
Policy 060111. Installing Virus Scanning Software.
"Anti Virus software must be chosen from a proven leading supplier."

8.4.1

Policy 030601. Restarting or Recovering your System.
"Information system owners must ensure that adequate back up and system recovery procedures are in place."

Policy 030603. Managing Backup and Recovery Procedures.
"Backup of the organisation’s data files and the ability to recover such data is a top priority. Management are responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business."

Policy 030604. Archiving Information.
"The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved."

Policy 030605. Archiving Electronic Files.
"The archiving of electronic data files must reflect the needs of the business and also any legal and regulatory requirements."

Policy 030606. Recovery and Restoring of Data Files.
"Management must ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files; especially where such files may replace more recent files."

8.4.3

Policy 010702. Recording and Reporting Hardware Faults.
“All information system hardware faults are to be reported promptly and recorded in a hardware fault register.”

Policy 010712. Damage to Equipment.
“Deliberate or accidental damage to organisation property must be reported to the nominated Information Security Officer as soon as it is noticed.”

Policy 030213. Responding to System Faults.
"Only qualified and authorised staff or approved third party technicians may repair information system hardware faults."

Policy 040208. Recording and Reporting Software Faults.
“Software faults are to be formally recorded and reported to those responsible for software support / maintenance.”

8.6.1

Policy 010301. Controlling IT Consumables.
“IT Consumables must be purchased in accordance with the organisation's approved purchasing procedures with usage monitored to discourage theft and improper use.”

8.6.2

Policy 030711. Shredding of Unwanted Hardcopy.
"All documents of a sensitive or confidential nature are to be shredded when no longer required. The document owner must authorise or initiate this destruction."

Policy 030903. Using External Disposal Firms.
"Any third party used for external disposal of the organisation's obsolete equipment and material must be able to demonstrate compliance with this organisation’s Information Security Policies and also, where appropriate, provide a Service Level Agreement which documents the performance expected and the remedies available in case of non compliance."

Policy 040301. Disposing of Software.
“The disposal of software should only take place when it is formerly agreed that the system is no longer required and that its associated data files which may be archived will not require restoration at a future point in time.”

8.6.3

Policy 030502. Managing Data Storage.
"Day-to-day data storage must ensure that current data is readily available to authorised users and that archives are both created and accessible in case of need."

Policy 030512. Linking Information between Documents and Files.
"Highly sensitive or critical documents must not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports must be self contained and contain all the necessary information."

Policy 030701. Managing Hard Copy Printouts.
"Hard copies of sensitive or classified material must be protected and handled according to the distribution and authorisation levels specified for those documents."

Policy 030702. Photocopying Confidential Information.
"All employees to be aware of the risk of breaching confidentiality associated with the photocopying (duplication) of sensitive documents. Authorisation from the document owner should be obtained where documents are classified as Highly Confidential or above."

Policy 030703. Filing of Documents and Information.
"All information used for, or by the organisation, must be filed appropriately and according to its classification."

Policy 030704. The Countersigning of Documents.
"Documents should be countersigned (either manually or electronically) to confirm their validity and integrity; especially those which commit or oblige the organisation in its business activities."

Policy 030705. Checking Document Correctness.
"Documents should be checked to confirm their validity and integrity; especially those which commit or oblige the organisation in its business activities."

Policy 030706. Approving Documents.
"All written communications sent out by the organisation to third parties are to be approved by authorised persons."

Policy 030707. Verifying Signatures.
"All signatures authorising access to systems or release of information must be properly authenticated."

Policy 030708. Receiving Unsolicited Mail.
"Unsolicited mail should not receive serious attention until and unless the sender's identity and authenticity of the mail have been verified."

Policy 030709. Style and Presentation of Reports.
"An agreed 'corporate' document style should be used which promotes consistency, integrity and promotes the agreed 'image' of the organisation."

Policy 030712. Using Good Document Management Practice.
"All users of information systems must manage the creation, storage, amendment, copying and deletion / destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary will be applied by management and determined by the classification of the information / data in question."

Policy 140103. Storing and Handling Classified Information.
"All information, data and documents must be processed and stored strictly in accordance with the classification levels assigned to that information."

8.6.4

Policy 010601. Managing and Using Hardware Documentation.
"Hardware documentation must be kept up-to-date and readily available to the staff who are authorised to support or maintain systems."

Policy 030207. Managing System Documentation.
"System documentation is a requirement for all the organisation's information systems. Such documentation must be kept up-to-date and be available."

Policy 050104. Controlling Program Listings.
"Program listings must be controlled and kept fully up to date at all times."

Policy 050401. Documenting New and Enhanced Systems.
"All new and enhanced systems must be fully supported at all times by comprehensive and up to date documentation. New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available."

8.7.2

Policy 030710. Transporting Sensitive Documents.
"The designated owners of documents which contain sensitive information are responsible for ensuring that the measures taken to protect their confidentiality, integrity and availability, during and after transportation / transmission, are adequate and appropriate."

8.7.3

Policy 030309. Developing a Web Site.
"Due to the significant risk of malicious intrusion from unauthorised external persons, Web sites may only be developed and maintained by properly qualified and authorised personnel."

Policy 030313. Giving Information when Ordering Goods on Internet.
"Staff authorised to make payment by credit card for goods ordered on the Internet, are responsible for its safe and appropriate use."

Policy 030314. 'Out of the Box' Web Browser Issues.
"Web browsers are to be used in a secure manner by making use of the built-in security features of the software concerned. Management must ensure that staff are made aware of the appropriate settings for the software concerned."

Policy 030315. Using Internet 'Search Engines'.
"Information obtained from Internet sources should be verified before used for business purposes."

Policy 030316. Maintaining your Web Site.
"The Web site is an important marketing and information resource for the organisation, and its safety from unauthorised intrusion is a top priority. Only qualified authorised persons may amend the Web site with all changes being documented and reviewed."

Policy 030805. Handling of Customer Credit Card Details.
"Customer credit card details entrusted to the organisation must be afforded a combination of security measures (technology and procedural) which, in combination, prevent all recognised possibilities of the card details being accessed, stolen, modified or an any other way divulged to unauthorised persons."

Policy 100101. Structuring E-Commerce Systems including Web Sites.
" e-commerce processing systems including the e-commerce Web site(s) are to be designed with protection from malicious attack given the highest priority."

Policy 100102. Securing E-Commerce Networks.
"e-commerce related Web site(s) and their associated systems are to be secured using a combination of technology to prevent and detect intrusion together with robust procedures using dual control, where manual interaction is required."

Policy 100103. Configuring E-Commerce Web Sites.
"The organisation's e-commerce Web site(s) must be configured carefully by specialist technicians to ensure that the risk from malicious intrusion is not only minimised but that any data captured on the site, is further secured against unauthorised access using a combination of robust access controls and encryption of data."

Policy 100104. Using External Service Providers for E-Commerce.
"Where third parties are involved in e-commerce systems and delivery channels, it is essential that they are able to meet the resilience and Information Security objectives of the organisation."

8.7.6

Policy 030313. Giving Information when Ordering Goods on Internet.
"Staff authorised to make payment by credit card for goods ordered on the Internet, are responsible for its safe and appropriate use."

Policy 030314. 'Out of the Box' Web Browser Issues.
"Web browsers are to be used in a secure manner by making use of the built-in security features of the software concerned. Management must ensure that staff are made aware of the appropriate settings for the software concerned."

Desarrollo y Mantenimiento de Sistemas.

10.1.1

Policy 040204. Interfacing Applications Software / Systems.
"Developing Interfacing software systems is a highly technical task and should only be undertaken in a planned and controlled manner by properly qualified personnel."

Policy 050201. Software Development.
"Software developed for or by the organisation must always follow a formalised development process which itself is managed under the project in question. The integrity of the organisation's operational software code must be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures."

Policy 050204. Justifying New System Development.
"The development of bespoke software is only to be considered, if warranted by a strong Business Case and supported both by management and adequate resources over the projected life time of the resultant project."

Policy 100101. Structuring E-Commerce Systems including Web Sites.
" e-commerce processing systems including the e-commerce Web site(s) are to be designed with protection from malicious attack given the highest priority."

10.2.2

Policy 030214. Managing or Using Transaction / Processing Reports.
"Transaction and processing reports should be regularly reviewed by properly trained and qualified staff."

10.2.3

Policy 030303. Sending Electronic Mail (E-mail).
"E-mail should only be used for business purposes, using terms which are consistent with other forms of business communication. The attachment of data files to an e-mail is only permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code."

Policy 030304. Receiving Electronic Mail (E-mail).
"Incoming e-mail must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code."

10.3.1

Policy 030205. Managing Electronic Keys.
"The management of electronic keys to control both the encryption and decryption of sensitive messages must be performed under dual control, with duties being rotated between staff."

10.4.1

Policy 030206. Managing System Operations and System Administration.
"The organisation's systems must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the organisation's information security."

Policy 050101. Managing Operational Program Libraries.
"Only designated staff may access operational program libraries. Amendments may only be made using a combination of technical access controls and robust procedures operated under dual control."

Policy 050106. Controlling Old Versions of Programs.
“Formal change control procedures with comprehensive audit trails are to be used to control versions of old programs.”

10.4.2

Policy 050302. Using Live Data for Testing.
“The use of live data for testing new system or system changes may only be permitted where adequate controls for the security of the data are in place.”

10.4.3

Policy 050102. Managing Program Source Libraries.
“Only designated staff may access program source libraries. Amendments may only be made using a combination of technical access controls and robust procedures operated under dual control.”

Policy 050104. Controlling Program Listings.
“Program listings must be controlled and kept fully up to date at all times.”

Policy 050105. Controlling Program Source Libraries.
“Formal change control procedures with comprehensive audit trails are to be used to control Program Source Libraries.”

10.5.1

Policy 030207. Managing System Documentation.
"System documentation is a requirement for all the organisation’s information systems. Such documentation must be kept up-to-date and be available."

Policy 030504. Permitting Emergency Data Amendment.
"Emergency data amendments may only be used in extreme circumstances and only in accordance with emergency amendment procedures."

Policy 030510. Setting up New Spreadsheets.
"The classification of spreadsheets must be appropriate to the sensitivity and confidentiality of data contained therein. All financial / data models used for decision making are to be fully documented and controlled by the information owner. "

Policy 030511. Setting up New Databases.
"Databases must be fully tested for both business logic and processing, prior to operational usage. Where such databases are to contain information of a personal nature, procedures and access controls must ensure compliance with necessary legislation e.g. Data Protection."

Policy 030515. Using Version Control Systems.
"Version control procedures should always be applied to documentation belonging to the organisation or its customers."

Policy 040201. Applying ‘Patches’ to Software.
“Patches to resolve software bugs may only be applied where verified as necessary and with management authorisation. They must be from a reputable source and are to be thoroughly tested before use.”

Policy 040202. Upgrading Software.
“Upgrades to software must be properly tested by qualified personnel before they are used in a live environment.”

Policy 040203. Responding to Vendor Recommended Upgrades to Software
“The decision whether to upgrade software is only to be taken after consideration of the associated risks of the upgrade and weighing these against the anticipated benefits and necessity for such change.”

Policy 050101. Managing Operational Program Libraries.
“Only designated staff may access operational program libraries. Amendments may only be made using a combination of technical access controls and robust procedures operated under dual control.”

Policy 050102. Managing Program Source Libraries.
“Only designated staff may access program source libraries. Amendments may only be made using a combination of technical access controls and robust procedures operated under dual control.”

Policy 050103. Controlling Software Code during Software Development.
“Formal change control procedures must be utilised for all changes to systems. All changes to programs must be properly authorised and tested before moving to the live environment.”

Policy 050105. Controlling Program Source Libraries.
“Formal change control procedures with comprehensive audit trails are to be used to control Program Source Libraries.”

Policy 050106. Controlling Old Versions of Programs.
“Formal change control procedures with comprehensive audit trails are to be used to control versions of old programs.”

Policy 050201. Software Development.
“Software developed for or by the organisation must always follow a formalised development process which itself is managed under the project in question. The integrity of the organisation’s operational software code must be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures.”

Policy 050202. Making Emergency Amendments to Software.
“Emergency amendments to software are to be discouraged, except in circumstances previously designated by management as 'critical'. Any such amendments must strictly follow agreed change control procedures.”

Policy 050205. Managing Change Control Procedures.
“Formal change control procedures must be utilised for all amendments to systems. All changes to programs must be properly authorised and tested in a test environment before moving to the live environment.”

Policy 050301. Controlling Test Environments.
“Formal change control procedures must be employed for all amendments to systems. All changes to programs must be properly authorised and tested in a test environment before moving to the live environment.”

Policy 050303. Testing Software before Transferring to a Live Environment.
“Formal change control procedures must be utilised for all amendments to systems. All changes to programs must be properly authorised and tested in a test environment before moving to the live environment.”

Policy 050305. Parallel Running.
“Normal System Testing procedures will incorporate a period of parallel running prior to the new or amended system being acceptable for use in the live environment. The results of parallel running should not reveal problems or difficulties which were not previously passed during User Acceptance Testing.”

10.5.2

Policy 040204. Interfacing Applications Software / Systems.
“Developing Interfacing software systems is a highly technical task and should only be undertaken in a planned and controlled manner by properly qualified personnel.”

Policy 040206. Operating System Software Upgrades.
“Necessary upgrades to the Operating System of any of the organisation’s computer systems must have the associated risks identified and be carefully planned, incorporating tested fall-back procedures. All such upgrades being undertaken as a formal project.”

Policy 040207. Support for Operating Systems.
“Operating Systems must be regularly monitored and all required 'housekeeping' routines adhered to.”

Seguridad Física y Ambiental.

7.1.1

Policy 120102. Securing Physical Protection of Computer Premises.
"Computer premises must be safeguarded against unlawful and unauthorised physical intrusion."

Policy 120202. Managing Remote Data Stores.
"Remote locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level."

7.1.2

Policy 020107. Securing Against Unauthorised Physical Access.
“Physical access to high security areas is to be controlled with strong identification and authentication techniques. Staff with authorisation to enter such areas are to be provided with information on the potential security risks involved.”

Policy 120104. Physical Access Control to Secure Areas.
"All computer premises must be protected from unauthorised access using an appropriate balance between simple ID cards to more complex technologies to identify, authenticate and monitor all access attempts."

Policy 120201. Managing On-Site Data Stores.
"On-site locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level."

Policy 120202. Managing Remote Data Stores.
"Remote locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level."

7.1.3

Policy 010501. Using Lockable Storage Cupboards.
“Sensitive or valuable material and equipment must be stored securely and according to the classification status of the information being stored.”

Policy 010502. Using Lockable Filing Cabinets.
“Documents are to be stored in a secure manner in accordance with their classification status.”
Policy 010503. Using Fire Protected Storage Cabinets.
“Documents are to be stored in a secure manner in accordance with their classification status.”

Policy 010504. Using a Safe.
“Documents are to be stored in a secure manner in accordance with their classification status.”

Policy 120103. Ensuring Suitable Environmental Conditions.
"When locating computers and other hardware, suitable precautions are to be taken to guard against the environmental threats of fire, flood and excessive ambient temperature / humidity."
Policy 120105. Challenging Strangers on the Premises.
"All employees are to be aware of the need to challenge strangers on the organisation's premises."

Policy 120201. Managing On-Site Data Stores.
"On-site locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level."

Policy 120202. Managing Remote Data Stores.
"Remote locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level."

7.1.4

Policy 030806. Fire Risks to Your Information.
"All data and information must be protected against the risk of fire damage at all times. The level of such protection must always reflect the risk of fire and the value and classification of the information being safeguarded."

Policy 120101. Preparing Premises to Site Computers.
"The sites chosen to locate computers and to store data must be suitably protected from physical intrusion, theft, fire, flood and other hazards."

Policy 120301. Electronic Eavesdropping.
" Electronic eavesdropping should be guarded against by using suitable detection mechanisms, which are to be deployed if and when justified by the periodic risk assessments of the organisation."

7.2.5

Policy 010403. Using Laptop/Portable Computers.
“Persons who are issued with portable computers and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimise the risks.”

Policy 010404. Working from Home or Other Off-Site Location (Tele-working).
“Off-site computer usage, whether at home or at other locations, may only be used with the authorisation of line management. Usage is restricted to business purposes, and users must be aware of and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures.”

Policy 010406. Using Mobile Phones.
“Personnel issued with mobile phones by the organisation are responsible for using them in a manner consistent with the confidentiality level of the matters being discussed.”

Policy 010703. Insuring Hardware.
“All computing equipment and other associated hardware belonging to the organisation must carry appropriate insurance cover against hardware theft, damage, or loss.”

Policy 010704. Insuring Laptops / Portables for use Domestically or Abroad.
“All portable computing equipment is to be insured to cover travel domestically or abroad.”

Policy 010708. Taking Equipment off the Premises.
“Only authorised personnel are permitted to take equipment belonging to the organisation off the premises; they are responsible for its security at all times.”

7.2.6

Policy 010701. Disposing of Obsolete Equipment.
“Equipment owned by the organisation may only be disposed of by authorised personnel who have ensured that the relevant security risks have been mitigated.”

7.3.1

Policy 010205. Using Centralised, Networked or Stand-Alone Printers.
“Information classified as Highly Confidential or Top Secret, may never be sent to a network printer without there being an authorised person to safeguard its confidentiality during and after printing.”

Policy 010503. Using Fire Protected Storage Cabinets.
“Documents are to be stored in a secure manner in accordance with their classification status.”

Policy 010504. Using a Safe.
“Documents are to be stored in a secure manner in accordance with their classification status.”

Policy 010705. Clear Screen Policy.
“All users of workstations, PCs / laptops are to ensure that their screens are clear / blank when not being used.”

Policy 010706. Logon and Logoff from your Computer.
“Approved login procedures must be strictly observed and users leaving their screen unattended must firstly lock access to their workstation or log off.”

Policy 020103. Securing Unattended Workstations.
“Equipment is always to be safeguarded appropriately - especially when left unattended.”

Policy 030811. Printing of Classified Documents.
"Information classified as Highly Confidential or Top Secret, may never be sent to a network printer without there being an authorised person to retrieve it and hence safeguard its confidentiality during and after printing."

Policy 030908. Using Clear Desk Policy.
"This organisation expects all employees to operate a clear desk policy."