Capítulo 1.- Marco teórico.

En este capítulo se hace una revisión de los conceptos básicos que son relevantes para la realización de este trabajo, además de hacer un análisis de plataformas de software y de hardware que ayuden a proponer una solución tecnológica para un servidor web y de bases de datos seguro en el CDMIT.

1.1.-Seguridad Informática.

La seguridad informática es un conjunto de protecciones (reglas, herramientas, recomendaciones, etc.) para salvaguardar la información, dispositivos y los procesos que forman parte de una red de datos.

Para poder brindar la seguridad deseada es necesario implementar herramientas y mecanismos de seguridad que ayuden a alcanzar el objetivo que es la seguridad de la información.

Se tienen que elegir las mejores herramientas y mecanismos para cumplir con el cometido de proporcionar robustez en cuanto a seguridad a la infraestructura de IT de la organización se refiere. Es necesario tener una serie de pasos que nos ayuden a contestar las siguientes preguntas:

a) ¿Qué es lo que se quiere proteger?

b) ¿De quiénes se van a proteger?

c) ¿Cómo se van a proteger?

Se deben seguir una serie de pasos que lleven a obtener las respuestas a las preguntas mencionadas y justamente en ese orden.

a) ¿Qué es lo que se quiere proteger?

A través de esta respuesta se identificarán los recursos a los que se requieren proteger y a lo que es denominado entorno de seguridad. En la implantación de un esquema de seguridad es necesario identificar los riesgos potenciales. Este proceso tiene que ser desarrollado formalmente por un grupo de todas las áreas de la organización, con el objeto de tener una visión más amplia sobre el valor de los activos y las consecuencias de que se vea comprometida la confidencialidad, integridad o disponibilidad. Para obtener está información es necesario contestar las siguientes preguntas:

- ¿Qué podría pasar?

  Esta pregunta tiene como objeto identificar los activos existentes para la compañía (software, hardware, datos, personas, etcétera) y los eventos amenazantes.

- ¿Si pasara, qué tan malo sería?

  Esta pregunta tiene como objeto cuantificar el impacto de las amenazas en todos los ámbitos (operativo, financiero, etcétera).

- ¿Qué tan frecuentemente podría pasar?

  Esta pregunta tiene como objeto cuantificar la frecuencia de ocurrencia potencial de los eventos amenazantes.

- ¿Qué tan correctas son las respuestas a las tres preguntas anteriores?

Con las respuestas anteriores se identifican claramente los activos sensibles para la empresa y las posibles consecuencias de que se vea comprometida la seguridad.

Con el estudio cuidadoso de las respuestas a estas preguntas, se podrá tener un nivel de conocimiento sobre los activos con que se cuenta y lo que representan para la organización, así como el conocer cuál sería el impacto en caso de que sufran algún incidente.

Para este trabajo, lo que se quiere proteger es el servidor web y de bases de datos del CDMIT.

b) ¿De quiénes se van a proteger?

Al resolver esta pregunta se identifican las amenazas, los riesgos y las vulnerabilidades a las que se encuentra expuesto el entorno identificado.

En una organización se garantiza la seguridad de la información que se maneja, determinando quienes son las personas autorizadas para manejar la misma, así como los recursos que necesita cada uno de los empleados para realizar las tareas que se le asignan.

La seguridad se enfoca en dar protección a los bienes que están expuestos a riesgos considerados como una potencial amenaza. Se debe prestar especial atención a las actividades maliciosas o a las actividades humanas, véase figura 1.1.

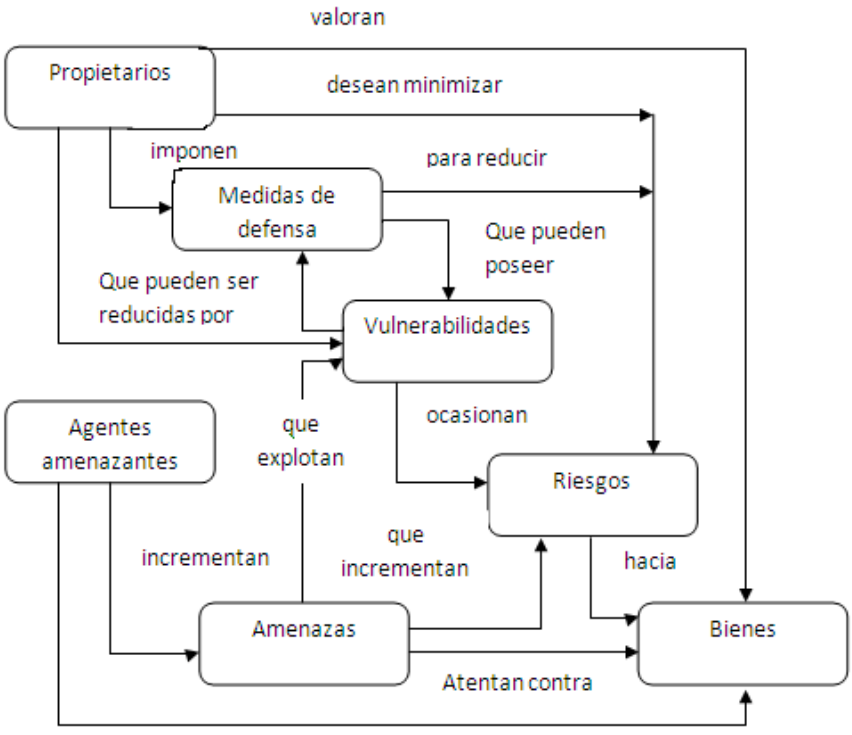

Figura 1.1.-Contexto y relaciones de la seguridad.

Los dueños, responsables o custodios son quienes estiman y valoran los bienes, que desean minimizar los riesgos informáticos implementando medidas de defensa para reducir las vulnerabilidades asociadas. Las amenazas también pueden estimar y valorar los bienes, además de buscar la forma de obtenerlos o abusar de ellos en forma contraria a los intereses de los propietarios.

Los dueños de los bienes, esto es, los propietarios, con ayuda de especialistas en seguridad informática, analizarán todas las amenazas que podrían presentarse para determinar únicamente cuáles son los que aplican a su entorno. Los resultados de este análisis se conocen como riesgos, y dicho análisis ayuda en la selección de las medidas de defensa para contrarrestarlos y reducir éstos a un nivel considerable.

Las medidas de defensa deben seleccionarse e implementarse para reducir puntos vulnerables y cumplir las políticas de seguridad de los dueños de los bienes. Después de la implantación de las medidas de defensa es posible que aún queden puntos vulnerables residuales, de manera que éstos pueden ser explotados por agentes amenazantes que representan un nivel mínimo de riesgo para los bienes; sin embargo es necesario que los dueños implementen restricciones adicionales para minimizar los riesgos.

Para este trabajo, la respuesta a esta pregunta se realizará con el análisis de riesgos de lo que se quiere proteger en el CDMIT.

c) ¿Cómo se van a proteger?

Las dos respuestas anteriores nos llevan a determinar las políticas de seguridad informática para el entorno analizado, ya que las normas ayudan a contrarrestar las amenazas y vulnerabilidades identificadas a fin de salvaguardar su entorno.

El plantear y dar respuestas a estas interrogantes será lo que nos dará la oportunidad de seleccionar de manera formal y segura las herramientas de seguridad necesarias para resguardar la información en riesgo.

Para este trabajo, la pregunta ¿qué es lo que se quiere proteger en el CDMIT? tiene como respuesta en este momento los servidores web y de bases de datos del CDMIT, la pregunta ¿de quiénes se van a proteger? se contestará con los resultados del análisis de riesgos que se explicará más adelante y por último, la pregunta ¿cómo se van a proteger? se resolverá con las políticas de seguridad.

A continuación se explicará el ciclo de la administración de la seguridad y la importancia que tiene para este trabajo.

1.2.- Administración de la seguridad.

Para que un esquema de seguridad quede completo, es necesario que se lleve a cabo la administración de la seguridad, véase figura 1.2. Para realizar esto se recomienda contar con un Departamento de Seguridad en Cómputo, el cual está conformado por personal que se encarga de cada área y por personal especializado en seguridad informática; así como la del equipo de trabajo que se encargará de administrar la seguridad informática.

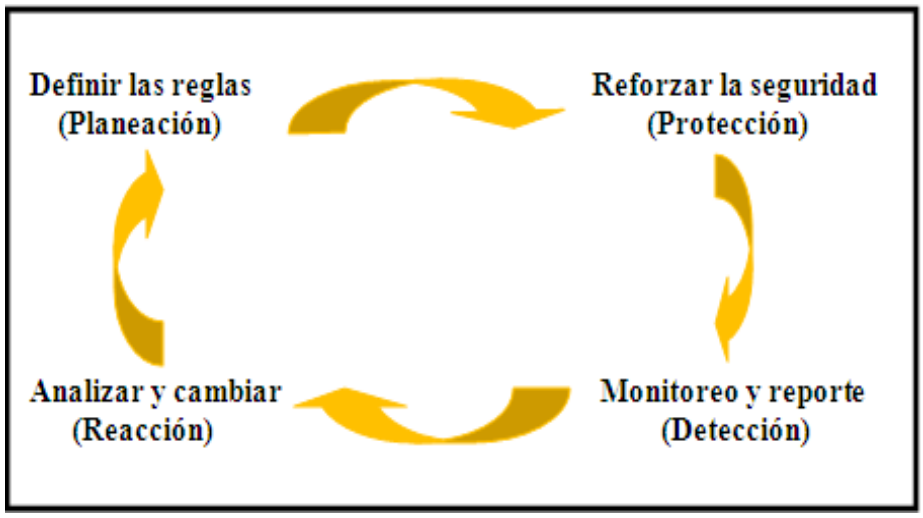

Figura 1.2.-Ciclo de la administración de la seguridad.

1.2.1.- Definición de administración de la seguridad.

La administración de la seguridad se refiere a gestionar y dirigir todas las acciones que se lleven a cabo con el fin de proteger la información, hacer uso lícito de ésta, así como de los recursos con los que cuenta la organización.

La administración consta de cuatro etapas que son:

Etapa 1: Planeación. Se debe llevar a cabo una revisión periódica de las políticas de seguridad, por lo que hay que revisar el esquema de seguridad desarrollado para identificar si se requiere actualizar, remover y modificar las que ya existen.

Etapa 2: Protección. Después de revisar y actualizar las políticas de seguridad del entorno, se debe de reforzar la seguridad con base en éstas y hacer uso de nuevas tecnologías, ya que estas nuevas formas de protección elevan el nivel de seguridad del entorno en cuestión.

Etapa 3: Detección. Es necesario contar con sistemas que permitan realizar actividades de monitoreo de forma continua y permanente en toda información, áreas y sistemas que sean considerados dentro de las políticas como de relevancia; y así mismo, generar reportes que permitan detectar alguna anomalía para tomar las medidas pertinentes, es decir, reaccionar a la anomalía.

Etapa 4: Reacción ante el incidente. En ésta etapa se toman las decisiones que dictan las acciones orientadas a salvaguardar los bienes informáticos de la empresa u organización, esto con base en la información obtenida de la etapa anterior, se realiza de manera continua un análisis de ésta para tomar una decisión de cambio de políticas o mecanismos. Estos cambios pueden ser desde actualizar la tecnología para llevar a cabo la protección de los bienes, modificar esquemas de seguridad o llevar a cabo una revisión extraordinaria de las políticas, entre otros.

Para que el esquema de seguridad del departamento de Cómputo del CDMIT este completo es necesario llevar a la práctica el ciclo de administración de la seguridad.

A continuación se explicará lo que es el análisis de riesgos, las metodologías que se tienen para realizar el análisis de riesgos y los tipos esenciales del análisis de riesgos para más adelante entender los resultados obtenidos de la realización del mismo.

1.3.- Definición de análisis de riesgos.

Se enuncian algunas definiciones de suma importancia para el análisis de riesgos:

- Activo. Es todo aquello que tiene valor para la organización y necesita protección.
- Riesgo. Todo aquello que representa la posibilidad de sufrir algún daño o pérdida.
- Aceptación del riesgo. Decisión para aceptar un riesgo.
- Análisis de riesgos. Uso sistemático de información disponible para identificar las fuentes y para estimar la frecuencia en la que determinados eventos no deseados pueden ocurrir y la magnitud de sus consecuencias.
- Manejo de riesgo. Proceso de identificación, control y minimización o eliminación de riesgos de seguridad – que pueden afectar a los sistemas de información – por un costo aceptable.
- Evaluación del riesgo. Comparación de los resultados de un análisis de riesgo con los criterios, estándares u otros criterios de decisión.
- Impacto. Pérdidas como resultado de la actividad de una amenaza (destrucción, modificación, revelación, denegación de servicios). El impacto generalmente se expresan en las áreas de impacto mencionadas.
- Pérdida esperada. El impacto anticipado y negativo a los activos debido a la manifestación de una amenaza.
- Amenaza. Todo aquello que puede, intenta o pretende destruir o dañar algo.

- Vulnerabilidad. Son las debilidades pertenecientes a algo.
- Ataque. La realización de una amenaza. Cuando una amenaza explota una vulnerabilidad y se logra el objetivo.
- Riesgo residual. Nivel de riesgo que queda después de la consideración de todas las medidas necesarias.
- Control. Protocolos y mecanismos de protección que permiten el cumplimiento de las políticas de seguridad de la organización.

1.3.1.-Tipos de Análisis de Riesgos.

Existen dos tipos de análisis de riesgos:

a) Cuantitativo.

Todos los activos, sus recursos y controles se identifican, y se evalúan en términos monetarios. Todas las amenazas potenciales se identifican y se estima la frecuencia de su ocurrencia, estas amenazas se comparan con las vulnerabilidades potenciales del sistema de tal forma que se identifiquen las áreas que son sensibles.

Esta metodología hace uso del término Expectativa de Pérdida Anual (ALE) o también llamado Costo Anual Estimado (EAC). La forma de calcularlo para un evento en concreto se realiza mediante la multiplicación de la ocurrencia de la amenaza por el valor del activo o clasificación del daño.

De esta forma se puede determinar si los controles existentes son adecuados o se requiere la implementación de otros, esto se observa cuando el producto obtenido tras multiplicar el valor del activo por la frecuencia de ocurrencia de la amenaza en un periodo de tiempo determinado por la duración del control es menos que el costo de dicho control.

Teóricamente es posible situar acontecimientos en el orden del riesgo ALE y posteriormente tomar las decisiones más convenientes. Los problemas de este tipo de análisis de riesgos se asocian generalmente a la falta de fiabilidad (probabilidad del buen funcionamiento de una cosa) y exactitud de los datos, debido a que es difícil lograr una figura representativa de la pérdida o daño que se tiene como resultado de las brechas de seguridad. La probabilidad raramente puede ser exacta y en algunos casos es capaz de promover la satisfacción personal. Además, los controles abordan acontecimientos potenciales que se correlacionan con frecuencia.

b) Cualitativo.

En esta otra metodología en lugar de establecer los valores exactos se asignan niveles de alto, bajo y medio que representan la frecuencia de ocurrencia y el valor de los activos. Este tipo de análisis es el consenso que debe realizarse para jerarquizar la información, los controles y decidir los valores, otra dificultad es la comparación de la pérdida potencial con el costo de implementación de controles para minimizarla, así como qué tan factible resulta aplicar los controles y en qué niveles de información.

Ambos análisis de riesgos hacen uso de tres elementos interrelacionados:

Amenazas

Son aquellos eventos que pueden causar daño a algo y están siempre presentes en cada sistema.

Vulnerabilidades

Son todos aquellos puntos de un sistema que están propensos a ser explotados por una amenaza y que pueden desencadenar en que dicha amenaza tenga mayor probabilidad de tener éxito.

Controles

Son las medidas precautorias que se toman para contrarrestar los ataques y reducir las vulnerabilidades. Existen cuatro tipos de controles:

- Los controles disuasivos reducen la probabilidad de un ataque deliberado.
- Los controles preventivos protegen vulnerabilidades haciendo que los ataques fracasen o que reduzcan su impacto.
- Los controles correctivos reducen el efecto de un ataque.
- Los controles detectores descubren ataques y disparan controles preventivos o correctivos.

Estos tres elementos pueden ser ilustrados mediante un modelo relacional simple que se aprecia en la figura 1.3.

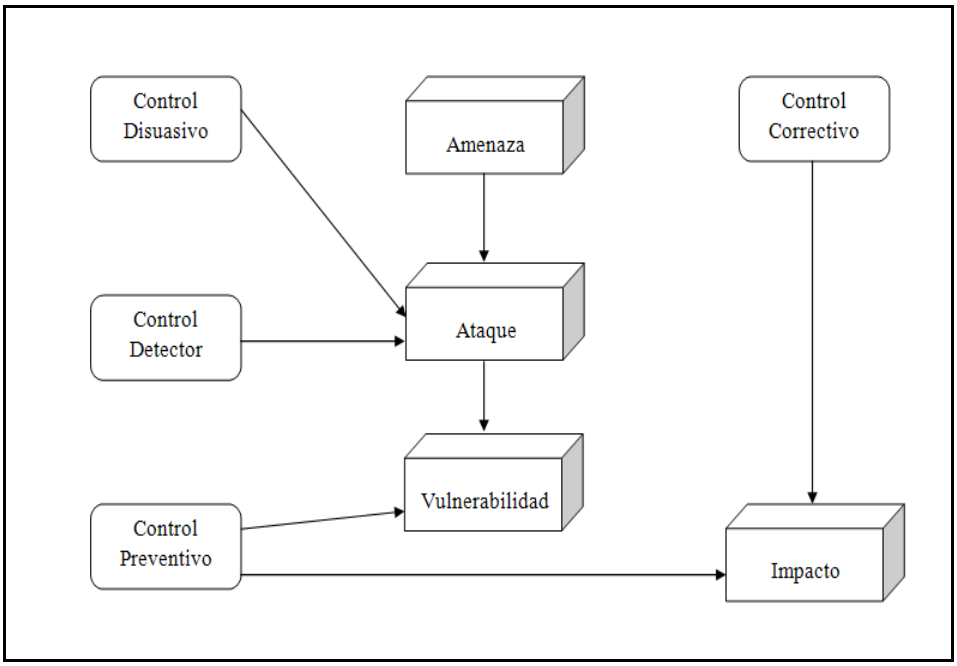

Figura 1.3.-Modelo relacional simple.

En el presente trabajo se hará el análisis cualitativo.

1.3.2.-Pasos a seguir para realizar un análisis de riesgo de tipo cualitativo.

El proceso del análisis de riesgos consiste en 8 pasos interrelacionados:

1. Identificar y evaluar los activos.

   El primer paso para todas las evaluaciones del riesgo es identificar los activos y asignar un valor a los activos que necesitan protección. El valor del activo es importante en la toma de decisiones para realizar cambios operacionales o incrementar la protección de los activos. El valor del activo se basa en su costo, sensibilidad, misión crítica o la combinación de estas propiedades. Así como determinar la importancia de los activos que tiene la organización.

2. Identificar las amenazas correspondientes.

   Después de identificar los activos que requieren protección, es necesario identificar y examinar las amenazas para determinar la posible pérdida si dichas amenazas se presentan.

3. Identificar y describir vulnerabilidades.

   El nivel de riesgo se determina analizando la relación entre las amenazas y las vulnerabilidades. Existen áreas de alta vulnerabilidad que no tienen consecuencias si

no se presentan amenazas. Un riesgo existe cuando una amenaza tiene una vulnerabilidad correspondiente.

4. Determinar el impacto de ocurrencia de una amenaza.

Cuando una amenaza explota una vulnerabilidad los activos sufren algún daño (cierto impacto). Las pérdidas son catalogadas en áreas de impacto llamadas:

- Revelación. Cuando la información es procesada y se pierde la confidencialidad.
- Modificación. El ataque cambia el estado original del archivo.
- Destrucción. Cuando el activo deja de funcionar completamente.
- Denegación de servicio. Pérdida temporal de los servicios.

5. Controles en el lugar.

Identificar los controles. Existen dos tipos que son:

- Controles requeridos. Todos los controles están basados en reglas y procedimientos. La clasificación de los datos almacenados y procesados en un sistema o red y su operación determinan que reglas aplicar, y éstas indican cuales son los controles.
- Controles discrecionales. Elegido por alguien comúnmente los administradores. Muchos de los controles requeridos no reducen el nivel de vulnerabilidad a un nivel aceptable.

6. Determinar los riesgos residuales.

Determinar cuál es el riesgo residual, si es aceptable o no. El riesgo residual toma la forma de las conclusiones alcanzadas en el proceso de evaluación. Las conclusiones deben identificar las áreas que tienen alta vulnerabilidad junto con la probabilidad de ocurrencia de una amenaza y todos los controles que no están dentro del lugar.

7. Identificar los controles adicionales.

Se identifica la forma más efectiva y menos costosa para reducir el riesgo a un nivel aceptable.

8. Preparar un informe del análisis de riesgos. En este informe se detallan los resultados obtenidos del análisis de riesgos así como las recomendaciones para evitar los riesgos.

Una vez que se ha realizado el análisis de riesgos el siguiente paso a desarrollar son las políticas de seguridad para tener una mejor administración de los recursos y del personal de la organización para evitar riesgos.

1.4.-Políticas de Seguridad.

Toda organización, tiene la necesidad y porqué no, la obligación de definir políticas de seguridad.

La necesidad surge porque existe un fallo o deficiencia en la seguridad de la información, la cual pone en riesgo a la misma y a la seguridad a la hora de proteger los datos, que implican significantes sumas de dinero y tiempo invertido.

Con buenas políticas se informa con mayor nivel de detalle a los usuarios, empleados y gerentes de las normas y mecanismos que deben cumplir y utilizar para proteger los componentes de los sistemas de la organización.

El estándar ISO 17799 contiene diez secciones de seguridad. Cada sección cubre un asunto o área, las cuales son utilizadas como base para la determinación de los riesgos de seguridad y la aplicación de controles de seguridad para el manejo de la seguridad de la información. La que se menciona a continuación es laque corresponde a las políticas de seguridad.

Las políticas de seguridad son un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad de la información dentro de la misma.

Las políticas definen la seguridad de la información en el sistema central de la organización, por lo tanto, un sistema central es seguro si cumple con las políticas de seguridad impuestas para esa organización. Las políticas de seguridad especifica qué propiedades de seguridad el sistema debe de proveer. De manera similar, las políticas definen la seguridad informática para una organización, especificando tanto las propiedades del sistema como las responsabilidades de seguridad de las personas.

Esta primera sección trata la administración, el compromiso y la dirección para lograr las metas de seguridad de la información. El objetivo de esta sección es:

- Proporcionar a la dirección o administración ayuda para la seguridad de la información.

a) Documento de la política de la información: una política de seguridad debe ser especificada en un documento especial para el propósito de ser cumplida, redactada en un lenguaje natural, claramente y sin ambigüedades posibles. El documento debe especificar cuáles son las metas de seguridad de la organización, qué propiedades de seguridad se pretenden cubrir con la aplicación de las políticas y la manera de usarlas. Este documento, junto con una jerarquía de estándares, principios y procedimientos, ayuda a implementar y reforzar los enunciados de la política, además de aprobarse por la administración, publicarse y comunicarse, de manera apropiada a todos los empleados, también debe expresar el compromiso y la aproximación de la organización para manejar la seguridad de la información.

b) Propiedad y análisis: el compromiso de administración de seguridad de la información se establece al asignar planes de propiedad y análisis del documento de

la política de seguridad de la información. La política debe tener un propietario, éste es el responsable de su mantenimiento y revisión periódica de acuerdo a un proceso definido, dicho proceso debe asegurar una revisión periódica debido a los cambios que afectan la evaluación original del riesgo, por ejemplo, incidentes de seguridad, nuevas vulnerabilidades o cambios a la infraestructura técnica o de la organización.

Para este trabajo, las políticas de seguridad ayudarán a contrarrestar las amenazas y vulnerabilidades de los servidores web del CDMIT.

A continuación se explican los principios fundamentales que deben ser reflejados en las políticas de seguridad para que cumplan el fin para lo que fueron hechas.

1.4.1.-Principios fundamentales.

Las políticas de seguridad deben reflejar fielmente la misión, la visión de la organización y los principios fundamentales que se explican a continuación.

1. Responsabilidad individual. Las personas son responsables de sus actos.
2. Autorización. Se establecen las reglas de quién y de qué manera puede utilizar los recursos.
3. Mínimo privilegio. La gente debe estar autorizada única y exclusivamente para acceder a los recursos que necesita para hacer su trabajo.
4. Separación de obligaciones. Las funciones deben estar divididas entre las diferentes personas relacionadas a la misma función o actividad.
5. Auditoría. El trabajo y los resultados deben de monitorearse desde el inicio y hasta después de haber terminado.
6. Redundancia. La redundancia puede afectar el trabajo y la información porque se tienen múltiples copias guardadas con importantes registros y dichas copias frecuentemente son guardadas en diferentes lugares.
7. Reducción del riesgo. El costo de la aplicación debe ser proporcional al riesgo.

Una vez que se sabe lo que tienen que reflejar las políticas de seguridad, el paso que sigue es redactarlas.

1.4.2.-Ciclo de vida de las Políticas de Seguridad.

Las políticas de seguridad dentro de una empresa tienen un ciclo de vida. A continuación se explican los pasos de este ciclo; así como las recomendaciones para su redacción.

1. Definición de las políticas de seguridad.

Para la definición de las políticas se consideran las siguientes recomendaciones:

i) Conocer los activos que se quieren proteger en la organización.

ii) Se elije una filosofía básica de las dos existentes que son la prohibitiva y la permisiva, la primera dice que todo esta prohibido a excepción de lo que específicamente está permitido y la segunda, todo esta permitido a excepción de lo que específicamente está prohibido.

iii) Se redacten como estándares o como recomendaciones, de manera positiva, ser generales, que no sean ambiguas y difíciles de entender, que las políticas no lleven a malos entendidos, hostigamientos, discriminación, abusos, etcétera y que no cambien mucho con el tiempo.

iv) Establecer responsabilidades de control y se tiene que asignar un dueño a los recursos y a la información que debe protegerse.

Una vez que han sido definidas las políticas de seguridad:

2. Implementación de las políticas de seguridad.

   Poner en funcionamiento las políticas de seguridad que se redactaron.

3. Verificación del cumplimiento de las políticas de seguridad.

   Se verifica con ayuda de la capacitación inicial y continua de todos los usuarios sobre la concientización de la seguridad y su importancia, además del cumpliendo de las políticas.

4. Revocación de la política de seguridad.

   Se verifica si las políticas tienen que actualizarse, si se están cumpliendo o si deben eliminarse o si no se cumplen. El tiempo de verificación de las políticas lo propone la organización dependiendo de los cambios de la tecnología, de los procesos, de las personas y de la misma organización.

Una vez que se redactaron las políticas de seguridad el siguiente paso es elaborar un plan de contingencias, que para este trabajo, se dejará como una recomendación para el CDMIT, ya que involucran muchos aspectos donde se necesita la colaboración de todos los empleados y encargados del CDMIT.

1.5.- Plan de contingencias.

1.5.1.-Definición de plan de contingencias.

Todas las instituciones deberían contar con un plan de contingencias actualizado, ya que es una herramienta que elimina, transfiere, mitiga o acepta los riesgos. Este plan de contingencias se basa en el análisis de riesgos que realiza la empresa previamente.

El plan de contingencias es una estrategia que se constituye de un conjunto de recursos ideados que tienen el propósito de servir de respaldo para conseguir una restauración progresiva y oportuna de los servicios de una organización.

A su vez, un plan de contingencia cuenta con las medidas necesarias para garantizar que la organización continúe con sus operaciones y se trata de un programa de tipo preventivo y correctivo que indica las acciones que deben tomarse inmediatamente ante una eventualidad de incidentes, accidentes y/o estados de emergencias que pudieran ocurrir tanto en las instalaciones como fuera de ella.

Los objetivos del plan de contingencia son el de planificar y describir la capacidad para respuestas rápidas, requerida para el control de emergencias.

A continuación se hará una comparativa sobre las características de diversos sistemas operativos, servidores web, manejadores de bases de datos y plataformas de hardware para poder elegir cada una de estás opciones para instalar un servidor web de acuerdo a los recursos económicos disponibles y el uso que se le va a dar al servidor web y de bases de datos.

1.6.-Sistemas Operativos para Servidores.

En el mercado existen diversos sistemas operativos especializados para funcionar como servidores, los más utilizados son los de las familias de Microsoft Windows o alguna distribución de Linux.

1.6.1.-Sistemas Operativos de la familia Microsoft.

La corporación estadounidense Microsoft es conocida mundialmente por el desarrollo del popular sistema operativo Microsoft Windows. Este sistema operativo ha evolucionado mucho desde la aparición de su primera versión en 1985 hasta tener toda una gama de productos orientados a cubrir las necesidades de los diferentes tipos de usuarios.

Actualmente Microsoft Windows cuenta con versiones para usuarios domésticos, para empresas y para dispositivos móviles.

1.6.1.1.-Microsoft Windows Server.

El sistema operativo Microsoft Windows Server cuenta con tres versiones recientes que se pueden encontrar en muchas organizaciones, nos referimos a las versiones 2000, 2003 y 2008.

En la tabla que se muestra abajo (tabla 1), podemos apreciar algunas características importantes de estas tres versiones de Microsoft Windows Server.

Característica.	Microsoft Windows 2000 Server.	Microsoft Windows Server 2003.	Microsoft Windows Server 2008.
Sistema de Archivos.	FAT 32 y NTFS.	NTFS.	NTFS.
Soporte HTTP.	Si.	Sí	Sí.
Soporte DNS.	Sí.	Sí.	Sí.
Soporte FTP.	Sí.	Sí.	Sí.
Soporte HTTPS.	Sí.	Sí.	Sí.
Soporte SSH.	Sí.	Sí.	Sí.
Soporte DHCP	Sí.	Sí.	Sí.
Soporte RAID.	Sí.	Sí.	Sí.
Fecha de lanzamiento.	Febrero 2000.	2003.	Febrero 2008.
Versión estable.	SP4.	R2.	SP2.
Precio promedio.	$199-$5,999 USD	$199-$7,999 USD	$199-$9,750 USD
Soporte.	Sólo Actualizaciones de Seguridad.	Sí.	Sí.
Licencia.	Propietaria.	Propietaria.	Propietaria

Tabla 1. Comparativa de Sistemas Operativos de la Familia Microsoft Windows Server.

Microsoft Windows 2000 Server es un sistema operativo ya obsoleto con respecto a las versiones 2003 y 2008. Ya no cuenta con soporte por parte de Microsoft, aunque aún cuenta con actualizaciones de seguridad.

El sistema operativo Microsoft Windows Server 2003 ha disminuido su precio con la salida al mercado de la versión 2008 de este sistema operativo, aunque su precio aún sigue siendo alto con respecto a otros sistemas operativos en el mercado, ya que oscila entre los 199 y los 7,999 USD, según la versión que se requiera, pero cuenta con nuevas herramientas con las que no contaba Microsoft Windows 2000 Server, como son IIS 6, Microsoft Identity Integration Server 2003 (MIIS), implementación de estándares abiertos (IEEE 802.1X), entre otras.

Microsoft Windows Server 2008 es el sistema operativo más reciente para servidores que ha sacado al mercado Microsoft, por lo que cuenta con todo el soporte y respaldo de Microsoft. Si se compara con otros sistemas operativos, su costo es muy elevado, ya que según la versión que se quiera, va desde los 199 hasta los 9,750 USD. Entre las novedades que se presentan respecto a la versión 2003 tenemos IIS 7, Windows Communication Foundation, Windows SharePoints Services, Security Configuration Wizard (SCW) y Network Access Protection, entre otras.

1.6.2.-Sistemas Operativos de la familia Linux.

El sistema operativo Linux cuenta con muchas distribuciones, algunas de las cuales son: Mandriva, Debian, Red Hat, SuSE, Gentoo, Ubuntu, Fedora, BSD, entre otras. Las distribuciones que cuentan con versiones especializadas en servidores y que son más utilizadas son Red Hat, SuSE, Ubuntu (basado en Debian) y Fedora (basado en Red Hat).

1.6.2.1.-Comparativa entre distribuciones del Sistema Operativo Linux.

Fedora es un Sistema Operativo Linux que cuenta con una amplia aceptación por parte de la industria, con lo último y lo más nuevo en software libre y de código abierto. Su versión actual a Diciembre de 2009 es la versión 12.

Ubuntu Server también es una distribución Linux que va ganando adeptos como Sistema Operativo para servidores. Cuenta con una gran cantidad de repositorios de software y actualmente se encuentra en su versión 9.10.

Por su parte Red Hat (la distribución en la que se basa Fedora), es una distribución de Linux ya probada y con un amplio mercado en la industria, cuenta con un soporte continuo y amplio que permite a las empresas implementar las soluciones que requieren de una manera robusta. La versión actual de Red Hat Enterprise Linux es la 5.3.

Finalmente otra distribución de Linux muy utilizada para el servicio web y de bases de datos es SuSe Linux, que es una distribución desarrollada por la compañía Novell, cuenta con herramientas muy poderosas que facilitan la gestión de paquetes, además de una gran capacidad de integración con tecnologías de Microsoft Windows, su versión actual es SuSE Linux Enterprise Server 11.

En la tabla 2 hacemos una comparativa de las características más importantes de las distribuciones de Linux más utilizadas para servidores.

Característica.	Fedora Core.	Ubuntu Server.	Red Hat Enterprise	SuSe Linux Enterprise Server
Sistema de Archivos.	Ext3.	Ext3.	Ext3.	Ext3.
Versión Actual.	12	9.10	5.3	11
Licencia	GPL.	GPL.	Propietaria	Propietaria
Precio Promedio.	Gratuito.	Gratuito.	$349.00 USD - $18,000.00 USD	$349.00 USD - $4,050.00 USD
Principales Servicios.	HTTP, FTP, SSH, DNS, DHCP,	HTTP, FTP, SSH, DNS, DHCP,	HTTP, FTP, SSH, DNS, DHCP,	HTTP, FTP, SSH, DNS, DHCP,

	HTTPS.	HTTPS.	HTTPS.	HTTPS.
Versión Estable.	11	9.04	5.3	11

Tabla 2. Comparación de los sistemas operativos de la familia Linux.

La distribución Fedora Core es completamente gratuita, está basada en la distribución Red Hat, pero a diferencia de ésta, es soportada por la comunidad, lo que puede ser una desventaja, ya que las actualizaciones, modificaciones y correcciones a fallos suelen tardar mas tiempo en aparecer que en un sistema operativo soportado por una corporación. Otra desventaja es que su manejo no es tan sencillo para usuarios con un nivel de conocimiento básico en Linux.

Ubuntu Server es otra distribución de Linux basada en Debian, completamente gratuita y que cuenta con un gran repositorio de software. Por defecto no incluye entorno gráfico, aunque es posible instalarlo y configurarlo. Este sistema operativo es soportado por la comunidad. Tiene gran aceptación a nivel mundial por su gran facilidad de uso, incluso para personas con conocimientos básicos en Linux. Es bastante rápido y se puede ejecutar en computadoras con bajos recursos. Además de ofrecer actualizaciones automáticas de manera constante.

El sistema operativo Red Hat Enterprise es una distribución de Linux de código abierto, que sin embargo no es gratuita, pero cuenta con actualizaciones continuas y un gran soporte por parte de la corporación que lo desarrolla. Es ampliamente utilizado en un sin fin de empresas medianas y grandes, ya que ofrece soluciones robustas y acordes a las necesidades de la mayoría de las empresas. Cuenta además con una integración muy buena con sistemas de las familias Windows y Unix.

SuSE Linux Enterprise Server es otra distribución de Linux que también es de código abierto y al igual que Red Hat Enterprise no es gratuita, pero cuenta con el soporte de Novell y con una amplia integración con sistemas operativos de Microsoft, ya que Novell y Microsoft han trabajado para ello. Esto representa una gran ventaja para las empresas que combinan ambas tecnologías, ya que hace más fácil, más rápido y menos costoso este proceso.

El conocer los tipos de sistemas operativos que hay en el mercado nos da la pauta para elegir la mejor plataforma para el servidor dependiendo de las necesidades del CDMIT y los recursos con los que cuenta.

1.7.-Servidores web.

En la actualidad existen una gran cantidad de servidores web, pero los más populares y utilizados son sin duda alguna Apache HTTP Server de Apache Software Foundation y Microsoft IIS de Microsoft Corporation.

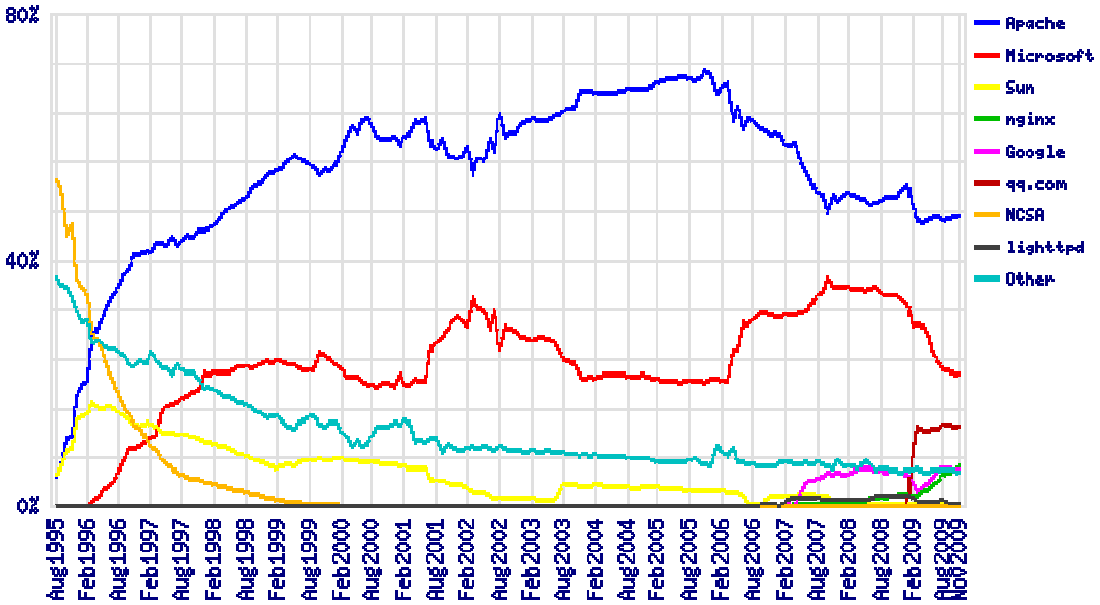

Figura 1.4.- Distribución mundial del uso de servidores web según Netcraft.

Apache es un servidor web creado por Apache Software Foundation y es el más utilizado en el mundo. Según Netcraft, a noviembre de 2009, Apache cuenta con cerca del 50% de usuarios en el mercado de servidores web.

El segundo servidor web más utilizado es IIS de Microsoft, el cual, además de proveer servicios web, tiene la capacidad de dar servicios de FTP y SMTP. Cifras de Netcraft indican que en el mercado IIS es utilizado por cerca del 35% de los usuarios de servidores web en el mundo (noviembre 2009).

1.7.1.-Comparativa entre Apache y IIS.

En la tabla 3 hacemos una comparativa entre Apache y IIS, en la cuál, pretendemos resaltar sus mejores características y ventajas para nuestras necesidades.

Característica.	Apache 1.X.	Apache 2.X.	IIS (HTTP).
Versión actual.	1.3	2.2	7.5
Versión estable.	1.3	2.0.3	7
Sistemas Operativos Compatibles.	Microsoft Windows, Linux, Novell NetWare, Solaris.	Microsoft Windows, Linux, Novell NetWare, Solaris.	Microsoft Windows.
Precio.	Gratuito.	Gratuito.	Gratuito.
Licencia.	GPL.	GPL.	Propietaria.
Soporte SSL-TLS.	Sí.	Sí.	Sí.
Principal ventaja.	Es compatible con múltiples plataformas.	Es compatible con múltiples plataformas.	Soporte nativo para ASP y ASP .NET.

Principal desventaja.	Con la aparición de la versión 2, se ha vuelto obsoleto.	Si no se tiene experiencia, resulta difícil de instalar y configurar.	Sólo es compatible con algunas versiones de Sistemas Operativos de Microsoft.

Tabla 3. Comparativa de los servidores web: Apache y IIS.

Con esta comparativa elegiremos el mejor servidor web de acuerdo a las necesidades del CDMIT.

1.8.-Manejadores de bases de datos.

En el mercado tenemos una gran cantidad de sistemas manejadores de bases de datos, algunos son de código abierto y otros son software propietario. Los de código abierto que son más conocidos son: MySQL, PostgreSQL y SQLite y los que son software propietario y que están más difundidos son: Microsoft SQL Server, Oracle, IBM DB2, IBM Informix y Sybase, entre otros.

En este punto sólo analizaremos 2 de los manejadores de bases de datos de código abierto, MySQL y PostgreSQL. Los manejadores con licencia propietaria son muy caros y llegan a alcanzar precios de entre $5,000 USD y $80,000 USD por licencia (por cada CPU).

1.8.1.-Comparativa entre MySQL y PostgreSQL.

A continuación mostramos la tabla comparativa de las características entre MySQL y PostgreSQL.

	MySQL.		**PostgreSQL.**
Característica.	MySQL Community Server.	MySQL Enterprise Server.	
Versión actual.	6.0	5.1	8.4.1
Versión estable.	5.1	5.1	8.4.1
Sistemas Operativos compatibles.	Windows, Linux, Solaris, FreeBSD, Mac OS X, HP-UX, IBM AIX, IBM i5/OS.	Windows, Linux, Solaris, FreeBSD, Mac OS X, HP-UX, IBM AIX, IBM i5/OS.	FreeBSD, Linux, Mac OS X, Solaris y Windows.
Precio.	Gratuito.	$599.00-$4,999.00 USD	Gratuito.
Licencia.	GPL.	Propietaria.	GPL.
Principal Ventaja.	Totalmente gratuito.	Soporte por parte de SUN.	Totalmente gratuito.

Principal desventaja.	No es posible realizar subconsultas.	Tiene un Costo muy alto.	Soportado por un menor número de plataformas que MySQL.

Tabla 4. Comparativa entre los manejadores de bases de datos: MySQL y PostgreSQL.

Se sabe que existen muchos manejadores de bases de datos pero con esta comparativa se podrá elegir el que más se adecue a las necesidades del CDMIT.

1.9.-Plataformas de Hardware.

Un aspecto muy importante a considerar para la seguridad en un servidor web y de bases de datos es también la plataforma de hardware en la cual será montado, ya que muchas veces si no se tiene el hardware con los recursos necesarios, resulta complicado ofrecer una seguridad robusta y garantizar la disponibilidad del servicio adecuadamente.

En esta sección hacemos una comparativa entre diferentes plataformas de hardware especializadas para el servicio web y de bases de datos. Analizamos un producto con características similares de tres de los mayores fabricantes de este tipo de hardware que ofrecen soluciones para servidores web en ambientes Linux y Windows, tal es el caso de IBM, Hp y Dell.

1.9.1.-Comparativa del hardware.

Para esta comparativa, se eligieron tres modelos de hardware para montar un servidor web y de base de datos con base en los 3 mayores distribuidores a nivel mundial para este tipo de productos en plataformas Linux y Windows: Dell Poweredge 1950 III, HP ProLiant serie BL260c G5 y IBM System x3200. Estos modelos, uno por fabricante, fueron elegidos de acuerdo a las recomendaciones hechas por los mismos fabricantes, ya que son productos apropiados para PyMES y que cumplen con las características necesarias para analizarlos en este trabajo (orientados a PyMES y a servicios web).

Característica.	Dell Poweredge 1950 III.	HP ProLiant serie BL260c G5.	IBM System x3200.
Procesadores compatibles.	Procesadores Intel Xeon.	Procesadores Intel Xeon.	Intel Xeon, Intel Pentium D.
Procesador.	Procesador Intel Xeon cuádruple; E5405, 2x6MB Cache, 2.0GHz, 1333MHz FSB.	Procesador Intel® Xeon® 445 Single-Core a 1,86 GHz.	Intel Xeon (doble núcleo) (4 MB/hasta 2,4 GHz/1066 MHz).
Número de núcleos soportados.	8	4	2
Sistemas operativos compatibles.	Microsoft Windows Server 2008, Microsoft Windows Server 2003, Red Hat Linux, Debian	Microsoft Windows Server 2003, Microsoft Windows Server 2008, Red Hat Enterprise	Microsoft Windows Server 2003, Microsoft Windows Server 2008, Red Hat Enterprise

	Linux, Ubuntu Linux, SuSE Linux, Novell Netware.	Linux, USE Linux Enterprise Server, Sun Solaris, Ubuntu Server Linux.	Linux, SUSE Linux Enterprise Server, Novell NetWare, IBM operating system 4690, Ubuntu Server.
Memoria RAM maxima.	64 GB.	48 GB.	8 GB
Memoria RAM.	Memorias DIMM 4GB, 667MHz, (4x1024MB).	1 GB (2 x 512 MB).	2 GB DDR II 667 or 800 MHz.
Capacidad máxima de almacenamiento en disco.	2 TB	2 TB.	2 TB.
Disco duro.	Disco duro de 250 GB, SATA, de 3.5 pulgadas, con velocidad de 7,200 RP.	Sin disco duro.	Sin disco duro.
Accesorios.	arjeta de interfaz de red Ethernet doble incorporada Broadcom® NetXtreme II 5708 Gigabit. 3 años de garantía.	1 adaptador de red adicional 10/100 dedicado a gestión iLO 2.	Integrated Gigabit Ethernet.
Temperatura idónea para el funcionamiento.	10 ºC-15ºC	Dato no disponible.	Dato no disponible.
Garantía.	3 años.	1 año.	3 años.
Precio aproximado.	$1,600.53 USD	$1,016.76 USD	$1,291.00 USD

Tabla 5. Comparativa de plataformas de Hardware.

Cabe señalar que el hardware anterior no cuenta con sistema operativo ni monitor.

Con todas las comparativas realizadas sobre las plataformas, servidores web, manejadores de bases de datos y del hardware nos será posible proponer la mejor solución web para cubrir las necesidades del CDMIT.

A continuación se explican las vulnerabilidades que tienen las aplicaciones web que ponen en riesgo a los servidores web y de bases de datos y también la forma de evitarlos para tener protegido al servidor, además de otros mecanismos de defensa.