CAPITULO 3

PROPUESTA METODOLÓGICA PARA EL ESTUDIO DE RIESGOS Y VULNERABILIDADES EN LA UPR.

3.1 PRESENTACIÓN

El trabajo que a continuación presentamos expone un análisis detallado del nivel de vulnerabilidad a que actualmente se hallan expuestos los bienes informáticos de la Universidad de Pinar del Río y al mismo tiempo proponemos el rediseño de la actual metodología en cuanto a la gestión de riesgos y detección de vulnerabilidades para lograr un mejor control y optimización de recursos.

Partiendo de nuestras convicciones de que una buena administración de riesgos en los bienes informáticos permitirá aprovechar todo el potencial tecnológico que posee la institución, presentamos el siguiente análisis metodológico.

3.2 INTRODUCCIÓN

Las áreas informáticas desde su creación han tenido un amplio reconocimiento técnico; sin embargo no se les ha tomado en cuenta en las grandes decisiones, por ello a pesar del inicial desarrollo que aún tiene el país en el empleo a gran escala de las tecnologías de la información, la realidad nos indica que se presentan las mismas amenazas y características a que se refiere toda la literatura sobre el tema que en países con mucha mayor experiencia y con mayor potencial tecnológico, tanto en los objetivos e impacto de los ataques a redes a nivel mundial, como en las causas y motivaciones de los presuntos atacantes.

Estas amenazas, desde el punto de vista de seguridad nacional, se pudieran definir como lo hacen el resto de los países del mundo aunque en el caso cubano

se potencian por la condición de país agredido por poderosos e inescrupulosos enemigos.

En Cuba, a pesar de que aún no se ha logrado alcanzar tales niveles de dependencia de la tecnología informática, diferentes eventos de seguridad reportados en las redes de las organizaciones estatales, de los que hemos tenido conocimiento, recomiendan de manera urgente estudiar y analizar la vulnerabilidad de los sistemas informáticos, todos los cuales (sin excepción) están expuestos a las más variadas y comprometidas amenazas.

Debido a lo anterior la Universidad de Pinar del Río al ser una Institución de Educación Superior moderna aprovecha las potencialidades del procesamiento informático, ello implica una nueva realidad, es decir, nuevos riesgos y por ende un mayor grado de vulnerabilidades en los sistemas y bienes de información de la institución.

Por lo tanto, el enfoque de este análisis metodológico se basa en el diagnóstico del ambiente informatizado y las posibles amenazas a las que se encuentran expuestos cada uno de los bienes, a partir una estrategia metodológica capaz de enfrentar y dar respuesta a los diferentes tipos de incidentes que puedan presentarse, tanto los que se originan desde el exterior, como los que tienen un carácter interno.

Todo esto ayudará a que la institución logre adecuados niveles de control para un mejor aprovechamiento de los recursos de información y una mejor administración en cuanto a bienes informáticos, basándonos en la metodología propia de la institución y trabajando en forma conjunta con los involucrados.

Conviene recordar que en la Universidad existen objetivos comunes entre todas las áreas en lo que respecta a los recursos informáticos, por ejemplo, el uso máximo y aprovechamiento de la tecnología mediante un buen uso de políticas, procedimientos y métodos apropiados; todo esto se verá reflejado en el análisis de riesgos y vulnerabilidades efectuado en la Universidad de Pinar del Río constituyéndose una herramienta básica para visualizar el cumplimiento de normas propias de la institución.

Consecuentemente proponemos una nueva visión a la actual metodología, la misma que tendrá como resultado un análisis de vulnerabilidad preciso de entender y comprender con valores reales, basados en un minucioso análisis obtenido en áreas estratégicas de la Institución y de esta manera emprender los esfuerzos necesarios para en una primera etapa poder corregir las debilidades que se detecten en los sectores claves y a la par que se proyecte una organización de alcance estratégico que involucre toda la Institución.

3.3 TECNICAS UTILIZADAS PARA EL DESARROLLO DEL ANALISIS INVESTIGATIVO EN LA UPR

Para el efecto descrito nos centraremos en una de las partes de la metodología **[Magerit, versión 1.0],** en donde se especifica las tareas a desarrollar, para el Análisis y Gestión de Riesgos de los Sistemas de Información.

3.3.1 Entrevistas

Las entrevistas son reuniones con una persona o un grupo de personas con el objetivo de recabar cierta información. Las entrevistas se dicen estructuradas cuando se atiene a una serie de preguntas planificadas sin margen para la improvisación. Las entrevistas se dicen libres cuando, existiendo un objetivo claro, no existe un formulario rígido.

En este análisis de gestión de riesgos se utilizó las entrevistas semi estructuradas en las que, existiendo un guión preestablecido de preguntas, el entrevistado tiene margen para extenderse en puntos no previstos o, más frecuentemente, responderlas en un orden diferente al previsto.

Tareas:

1. Determinar la oportunidad.- es casi imposible disponer de un cuestionario rígido, y el entrevistado debe disfrutar de una elevada flexibilidad.
2. En las tareas de descubrimiento como son (Identificación de bienes informáticos de la UPR), las entrevistas son semi-estructuradas, usando el cuestionario como guía que hay que adaptar.

3. En las tareas de detalle (evaluación, identificación, estimación de valores de riegos y amenazas de los bienes informáticos de la UPR), el margen de maniobra está fuertemente pautado, ya que en este punto nos enfocaremos a la Metodología actual de la UPR, usándose entrevistas estructuradas.

El mayor volumen de entrevistas se encuentran a partir de la tarea 2 del Análisis de riesgos, en el que hay que centrarse especialmente en las actividades de: Identificación, evaluación, identificación de amenazas y estimación de riesgos sobre los bienes informáticos en la UPR. éstas etapas permiten conocer los elementos objeto del análisis de riesgos, identificándolos, valorándolos y relacionándolos entre si.

Durante la preparación de la entrevista:

1. Recopilar los cuestionarios

2. Ubicar y localizar a los entrevistados, para optimizar la realización de las entrevistas

3. Confirmar cada entrevista, informando de los documentos que se van a requerir durante la entrevista, para facilitar su disponibilidad.

3.3.2 Reuniones

Las reuniones tienen como objetivo obtener información que se encuentra repartida entre varias personas, tomar decisiones estratégicas, tácticas u operativas, transmitir ideas sobre un determinado tema, analizar nuevas necesidades de información, así como comunicar los resultados obtenidos como consecuencia de un estudio.

Para realizar una reunión es necesario:

1. Designar a las personas que deben participar en ella
2. Determinar el lugar en el que poder llevarla a cabo.

3.3.3 Observación Directa

La observación directa se obtiene a través de la observación participante, es decir, formando parte del grupo estudiado.

3.4 OBJETIVOS DEL ESTUDIO DE VULNERABILIDAD

- Determinar el nivel de vulnerabilidad en los bienes informáticos de la UPR.
- Establecer las políticas que se requieran para minimizar los riesgos sobre los bienes informáticos.
- Realizar un análisis minucioso de los riesgos y amenazas que soportan los Sistemas de Información y redes de datos.

- Desarrollar una documentación actualizada de análisis de riesgos para posteriores estudios de riesgos de bienes informáticos en la UPR.

3.5 ALCANCE

El presente análisis comprende las principales áreas donde se alojan los bienes informáticos con los que cuenta la Universidad de Pinar del Río y se pretende mostrar en una forma cuantificable, la situación actual de riesgos y vulnerabilidades en cada uno de los recursos que forman parte de tecnología informática de esta Institución, señalando los fallos detectados y las posibles soluciones que ayuden a minimizar a un menor índice las vulnerabilidades de los bienes que son considerados de mucha importancia en estos tiempos, para así lograr la eficiencia administrativa de la entidad mencionada.

Para el análisis se considera lo siguiente:

3.5.1 Redes de diferentes tipos

3.5.1.1 Intranet

Red local que funciona dentro de esta Institución, utiliza herramientas de Internet la cual tiene como base el protocolo TCP/IP de Internet y utiliza un sistema firewall (cortafuegos) que nos permite acceder a la misma desde el exterior, el (**Anexo1)**,refleja el esquema topológico actual del cortafuegos de la UPR.

3.5.1.2 Extranet (Extended Intranets)

Estructura de comunicación resultante de la ampliación de la Intranet, que conecta a la Institución con los demás organismos, utilizando una red privada

virtual resultante de la interconexión de dos o más intranets mediante Internet como medio de transportar la información entre sus nodos.

3.5.1.3 Internet

Interconexiones entre *gateways,* se efectúan a través de diversas vías de comunicación entre las que figuran líneas telefónicas, fibras ópticas y enlaces satelitales

3.5.2 Otros tipos de redes de importancia

Atendiendo a la importancia que estos recursos poseen, describiremos los siguientes segmentos de red que forman parte de la UPR.

- Segmentos de red del Edificio de laboratorios.

  El croquis con la ubicación de las áreas que cubren el Nodo Central y los subnodos y la estructura de la red se presentan en el **(Anexo 2)**.

- Segmentos de red del Edificio Docente.

  Para un mejor entendimiento mostramos el esquema Topológico del Edificio Docente en el **(Anexo 3)**.

- Segmentos de red del Edificio de Residencia Estudiantil.

  Podremos observar su estructura en el **(Anexo 4).**

3.5.3 Sistemas automatizados de control de proceso

Se asumen los bienes informáticos que se encargan del control y la comunicación de los servicios centrales que utiliza la UPR. entre los cuales citaremos:

- Servidores Centrales y Nodo de Comunicación

3.5.4 Sistemas de gestión de datos de interés institucional.

Las reuniones realizadas en diferentes áreas de la Institución nos permiten situar varios sistemas automatizados, los mismos que son considerados como bienes propios de la Institución, entre los cuales podemos mencionar:

- Sistema **ASSET**
- Sistema **MICROCAMPUS**
- Sistema **Kuota**
- Plataforma **SEPAD**
- Sistema **ARINT**
- Sistema control de la **Divisa** (este sistema en la actualidad se encuentra descentralizado de los demás departamentos de la UPR**).**
- Sistema de Control de Estudiantes (Sistema que se encuentra en una etapa de implementación, motivo por el cual no será tomado en consideración en nuestro respectivo análisis)
- Sistema **TUNEL**
- Sistemas del Plan de Transporte.

3.5.5 Otro Tipo de Aplicaciones y Sistemas

Dentro de este grupo se especificarán los sistemas y aplicaciones que son de importancia para el funcionamiento de la UPR, respaldándonos en el criterio obtenido en una entrevista realizada a la Vicerrectora de Investigaciones, pero hay que aludir a que en nuestro análisis no constan estas aplicaciones, debido a que nuestro estudio está enfocado en una forma general como detalla la actual metodología universitaria, motivo por el cual planteamos que sean tomados en consideración en posteriores análisis de riesgos ya que ayudará en gran parte a

tener una visión mas detallada de los riesgos a los que se hallan expuestos los bienes informáticos. A continuación tenemos:

- Pagina Web Internet
- Pagina web Intranet
- Pagina Web de las Áreas
- Portal de la Biblioteca
- Anuario Científico de la **UPR**
- Tienda Virtual del GESAT

3.6 CUESTIONES BÁSICAS

Durante el desarrollo del este análisis se determinarán los siguientes aspectos:

- ¿Qué espacios deben ser considerados importantes? o sea, qué sectores o áreas sustentan su actividad en redes, sistemas o aplicaciones considerados como críticos para la Institución en general.
- ¿Cuáles son los riesgos y que amenazas que los provocan?
- ¿Cual es el valor actual y real en lo que se refiere al nivel de vulnerabilidad de los Bienes informáticos en la UPR?
- ¿Qué impacto podría esperarse?
- ¿Cómo manejar los posibles riesgos?

3.7 DETERMINACIÓN DE LAS NECESIDADES DE PROTECCIÓN

Las necesidades de protección se determinan mediante la realización de un análisis de riesgos, que es el proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos, e implica la

identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar dentro de la Universidad de Pinar del Río.

En el proceso de análisis de riesgos se pueden diferenciar dos aspectos:

3.7.1 La Evaluación de Riesgos, orientada a determinar todos los sistemas que en su conjunto o en cualquiera de sus partes, pueden verse afectados directa o indirectamente por amenazas, estimando todos los riesgos y estableciendo un valor real a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la Institución.

3.7.2 La Gestión de Riesgos, según lo que nos proponemos implica la identificación, selección, y diseño de las Políticas necesarias para eliminar y reducir los riesgos identificados en la UPR.

Aspectos a tener en cuenta:

- Reducir la probabilidad de que una amenaza ocurra.
- Limitar el impacto de una amenaza, si esta se manifiesta.
- Reducir o eliminar una vulnerabilidad existente.

La necesidad de realización de sucesivos análisis de riesgos estará determinada por las siguientes circunstancias:

- Los elementos que componen un sistema informático están sometidos a constantes variaciones: nuevas tecnologías, cambios de personal, nuevos locales, nuevas aplicaciones, nuevos servicios, etc.
- La aparición de nuevas amenazas o la variación de la probabilidad de ocurrencia de alguna de las existentes.

- Pueden aparecer nuevas vulnerabilidades, o variar, o incluso desaparecer alguna de las existentes, originando, modificando o eliminando posibles amenazas.

Sobre la base de lo anterior, es de mucha importancia mantener una actualización sistemáticamente de porcentajes en riesgos, y proponemos que se utilice el presente análisis de vulnerabilidades para consideraciones posteriores, lo que posibilitará que el tiempo y los medios necesarios para su realización sean menores y muy eficaces.

En resumen, durante la determinación de las necesidades de protección de los Bienes Informáticos es necesario:

a) Evaluar el estado actual de la seguridad.

b) Caracterizar el entorno informático.

c) Identificar las amenazas potenciales sobre los sistemas informáticos y estimar los riesgos sobre los mismos.

3.8 EVALUACION DEL ESTADO ACTUAL DE LA SEGURIDAD

Efectuando una revisión a la Metodología implantada en la Universidad de Pinar del Rió y por ende al Plan de seguridad Informática vigente, observamos que dicho plan no ha sido desarrollado en su plenitud, debido a que no constan determinados sistemas y aplicaciones que también son considerados bienes universitarios, a demás de esto observamos la existencia de determinados valores estimados en el análisis de riesgos, pero en ninguna parte del documento encontramos las evaluaciones de las personas a quienes fueron dirigidas o qué áreas fueron las involucradas para sustentar y respaldar el estudio, al analizar las políticas de seguridad informática pudimos apreciar un porcentaje considerable de incumplimiento de sus normas.

3.9 CARACTERIZACIÓN DEL ENTORNO INFORMÁTICO

La caracterización del entorno informático incluye la determinación de los bienes informáticos dentro de la Universidad de Pinar del Río que requieren ser protegidos, su valoración y clasificación según su importancia. Durante este proceso hay que considerar:

- Tecnologías utilizadas.
- Estructuración de las Redes instaladas dentro de la UPR
- Identificación de sistemas en explotación o aquellos que se encuentran en una etapa pasiva.
- Valoración y estimación de los posibles riesgos y amenazas a las que se hallan expuestas las tecnologías de información de la UPR.
- Otros datos de interés.
- Una vez identificados los bienes informáticos que la Institución necesita proteger es necesario determinar su importancia dentro de la misma y clasificarla según su categoría.

Para la determinación de valores sobre la importancia de los bienes informáticos hemos dado un seguimiento a los lineamientos de la Metodología para la Realización del Estudio de Vulnerabilidad de los sistemas Informáticos, orientada por la Carta Circular 31/2001 de Carlos Lage Dávila e implantada en la UPR, la misma que está descrita de forma numérica asignando valores entre cero y diez (0 si no tiene importancia y 10 sí es máxima).

La valoración de estos bienes informáticos posibilitará, mediante su categorización, determinar en que medida uno es más importante que otro y se realiza teniendo en cuenta aspectos tales como:

La descripción y función que realizan cada uno de los bienes informáticos; el costo, este punto proponemos tratarlo desde diferentes puntos de vista tanto en el sentido económico como también en su valor de uso, ya que un bien informático puede ser muy costoso económicamente y por ello considerado de importancia alta, pero también puede tener un costo mínimo pero su función o uso puede ser de vital importancia para la Institución, por todo esto exponemos en el análisis la siguiente fórmula para determinar un Costo Total que involucra estos dos aspectos.

Costo Total = Costo Valor + **Costo de Uso**

También se analiza la Imagen que este representa con el efecto que ocasionaría la pérdida del mismo, así como la Confidencialidad, la Integridad, la Disponibilidad de cada bien informático, y en una forma básica presentamos un nuevo aspecto a ser considerado en el estudio de riesgos y vulnerabilidades, como es la Función que desempeña cada bien dentro de la Institución.

Esta forma numérica tiene la ventaja de que permite estimar el nivel de riesgo con mayor rigor, así como la valoración por áreas o grupos de elementos más fácilmente, como se describe en el siguiente cuadro.

Importancia baja	0 a 3,5
Importancia media	3,6 a 5,9
Importancia alta	6,0 a 7,9
Importancia muy alta	8,0 a 10

3.10 DESARROLLO DEL ANÁLISIS DE RIESGOS EN BASE A LA PROPUESTA DE PERFECCIONAMIENTO PARA LOS BIENES INFORMÁTICOS DE LA UPR.

Con el propósito de obtener un adecuado entendimiento de las implicaciones que tiene el uso de esta nueva propuesta metodológica en amenazas y vulnerabilidades, se efectuaron entrevistas y reuniones con las personas encargadas de administrar los bienes informáticos, para lo cual consideramos en este trabajo cuatro grupos de gran importancia dentro de la Institución Educativa, por ser ejes primordiales del control de recursos de la información a nivel de toda la Institución, los mismos que nos proporcionaron la información necesaria para el desarrollo de este análisis metodológico:

Grupo A:

Grupo de Redes de la UPR.

Grupo B:

Dirección de Formación Científica de la UPR.

Grupo C:

Responsable de la Seguridad Informática de la UPR

Grupo D:

Vicerrectoría de Investigación y Postgrados.

Con los grupos anteriormente citados desarrollaremos el siguiente análisis de riesgos a los bienes informáticos que constituyen propiedad absoluta de la UPR**.**

3.11 IDENTIFICACION DE BIENES INFORMATICOS

La primera descripción corresponde a la identificación de los bienes informáticos fundamentales, su tipo, ubicación y como un aporte para un mejor entendimiento adicionaremos un nuevo aspecto denominado **Función**, éste nos permitirá explicar la tarea que realiza en una forma general.

Atendiendo a la información recopilada de los grupos considerados como críticos en la gestión de riesgos, presentaremos el diagnóstico total y actual e identificaremos todos los bienes de la Universidad de Pinar del Río, ver **Anexo (5)**, de los cuales los primeros once bienes fueron identificados por el Grupo A y los demás bienes fueron considerados por el Grupo B, Grupo C y Grupo D.

En el cual cada columna significa lo siguiente:

1. Número de orden consecutivo de los bienes informáticos.
2. Descripción de los bienes informáticos.
3. Tipo de bienes informáticos:

- RD Redes de diferentes tipo
- GD Sistemas de gestión de datos
- CP Sistemas de control de procesos
- OT Otros tipos de aplicaciones o sistemas

4. Ubicación de los bienes informáticos.
5. Función general que realiza cada bien informático.

TABLA 1: IDENTIFICACION GENERAL DE LOS BIENES INFORMATICOS EN LA UPR

No	DESCRIPCIÓN	TIPO	UBICACIÓN	FUNCION
1	Servidores Centrales y Nodo de Comunicación	CP	Edificio de Laboratórios, 2do piso	Comunicación y servicios centrales de la UPR
2	Segmentos de red de Edificio de laboratorios	RD	Edificio de Laboratórios, 2do piso.	Interconectar la diferentes áreas de UPR
3	Segmentos de red de Edificio Docente ()	RD	Edificio Docente	Interconectar la diferentes áreas de UPR
4	Segmentos de red de Edificio de Residencia Estudiantil ()	RD	Edificio de Residencia Estudiantil	Interconectar la diferentes áreas de UPR
5	Sistema **ASSET**	GD	Dpto. Economía y Contabilidad	Control Económico
6	Sistema **MICROCAMPUS** (Plataforma docente)	GD	Edificio de Laboratórios, 2do piso.	Plataforma virtual de soporte para la enseñanza
7	Sistema **Kuota**	GD	Edificio de Laboratórios, 2do piso.	Sistema de gestión para el acceso de Internet de los usuarios
8	Plataforma **SEPAD**	GD	Edificio de Laboratórios, 2do piso.	Sistema (Educación a distancia)
9	Sistema **ARINT**	GD	Edificio de Laboratorios 1er Piso	Relaciones Internacionales
10	Sistema **TUNEL**	GD	Edificio de Laboratórios, 2do piso.	Gestión de usuario de correo electrónico
11	Sistemas Automatización Ingreso de Educación Superior	OT	Edificio de Laboratorio	Procesamiento ordenado de la carreras de educación Superior
12	Sistemas ISIS	OT	Edificio de Laboratórios, 2do piso.	Registro y control de Libros

3.12 EVALUACION DE BIENES INFORMÁTICOS

En esta fase procedemos a realizar la valoración de la importancia de los bienes a partir de la función que estos cumplen, el costo total anteriormente analizado, la imagen que representa en la **UPR** y su comportamiento en relación a los aspectos de confidencialidad, integridad y disponibilidad en cada sistema de datos o redes.

En el **(Anexo 6),** mostramos el criterio individual de los Administradores de la red en la UPR. con relación a la evaluación de los bienes.

.En el **(Anexo 8)**, se detalla la evaluación dirigida a la Dirección Científica de investigación de la UPR.

En el (**Anexo 7)**, presentamos la evaluación del Responsable de la Seguridad Informática de la Institución

En el **(Anexo 9)**, se refleja la evaluación dirigida a la Vicerrectoría de Investigaciones y Postgrado de la UPR.
A partir de estas evaluaciones podemos representar valores cuantificables y totales sobre la importancia que tienen los bienes informáticos en toda la Institución.

En donde cada columna tiene el siguiente significado:

1. NÚMERO de orden consecutivo
2. DOMINIO: Identificación para agrupar bienes informáticos afines por las funciones que realizan y/o por la administración sobre ellos, se incrementarán de acuerdo a la cantidad que se crea necesaria.
3. FUNCIÓN: Importancia de la tarea que cumplen los bienes informáticos.
4. COSTO TOTAL: Valor económico y valor de uso de los bienes informáticos.

5. IMAGEN: Resultado interno y/o externo que produciría la pérdida de los bienes informáticos.
6. CONFIDENCIALIDAD: Necesidad de proteger la información que de los bienes informáticos pueda obtener.
7. INTEGRIDAD: Necesidad de que la información no se modifique o destruya.
8. DISPONIBILIDAD: Que los servicios que de bienes informáticos se esperan puedan ser obtenidos en todo momento de forma autorizada.
9. IMPORT. (Wi): Importancia de los bienes informáticos.

Los aspectos de Función, Costo Total, Imagen, Confidencialidad, Integridad y Disponibilidad, se le asignarán valores entre 0 y 10, (0 sino tiene importancia y 10 si es máxima) a partir de la estimación que se haga de la importancia de cada uno de estos factores sobre los bienes informáticos analizados.

Al estimar la IMAGEN hay que tomar en consideración el resultado que ocasionaría la pérdida de los bienes informáticos y se debe tener en cuenta el tiempo que la entidad puede seguir trabajando sin los mismos, lo que puede ser vital para su funcionamiento.

La Importancia (Wi) de los bienes informáticos se calcula por el promedio de los aspectos analizados, es decir, el resultado de la suma de las columnas 3 a 8 dividido por 6.

La suma total (Wt) de los valores (Wi) representa la importancia total de los bienes informáticos en la Institución.

$$Wt = W1 + W2 + ... + Wn$$

TABLA 2: EVALUACIÓN TOTAL DE LOS BIENES INFORMÁTICOS UPR

N0	DOM	VALORACIÓN POR ASPECTOS						IMPORTANCIA(Wi)
		FUNCIÓN	COSTO TOTAL	IMAGEN	CONFIDEN	INTEGRID	DISPONIBILIDAD	
1	D1	9,85	9,92	9,85	9.71	9,42	9,85	9,76
2	D2	8,7	8,62	9,27	6.98	8,41	8,27	8,37
3	D3	8,98	8,84	9,27	7,41	8,55	8,55	8,6
4	D4	8,27	8,48	8,41	7,7	8,7	8,27	8,30
5	D5	10	9.14	10	10	10	10	9.85
6	D6	8,7	6.80	8,27	7.27	8,41	8,98	8,07
7	D7	8,98	7,7	9.27	9,27	9,27	9,41	8,98
8	D8	6,12	8.12	7,12	6,12	6,41	8,27	7.02
9	D9	7,55	7,34	7,55	7,27	7,84	7,98	7.58
10	D10	9.12	7,62	8,84	9.55	8,84	8.84	8,80
11	D11	9.41	9.41	9.41	9.41	9.41	9.41	9.41
12	D12	8.3	7.13	4.63	1.96	4.63	4.63	5.21
13	D13	7.3	7.63	7.96	4.96	8,3	8,3	7.40
TOTAL								**107.35**

3.13 IDENTIFICACIÓN DE AMENAZAS Y ESTIMACIÓN DE RIESGOS

Una vez que los bienes informáticos que requieren protección son identificados y valorados según su importancia, es necesario identificar las amenazas sobre estos y estimar la pérdida que puede producir su materialización.

La identificación de amenazas corresponde a un análisis cruzado a partir del reconocimiento de cada una de las amenazas que pueden afectar a los bienes informáticos, su probabilidad de ocurrencia y el impacto que puedan producir dentro de la Institución En cada una de las filas de la tabla de Identificación de amenazas se describirán, numerándolas consecutivamente según su nivel de incidencia para su posterior identificación en la Tabla de Estimación de Riesgos y se abrirá una columna para cada bien informático, los cuales fueron identificados anteriormente en la Tabla 1 Identificación de Bienes de la UPR, a continuación procederá a marcar con una cruz la fila correspondiente a cada amenaza que incida sobre el bien.

3.13.1 IDENTIFICACIÓN DE AMENAZAS

Está dirigida a la identificación de las principales amenazas, activas en su mayoría y pasivas, que están sometidas la utilización de las Tecnologías de la Información y su posibilidad de acción sobre los bienes informáticos, para analizar estas amenazas se realizaron diálogos con los siguientes grupos :el Grupo de Redes de la UPR, ver **(Anexo 10),** Dirección de Formación Científica, ver **(Anexo 11)**, Responsable de la Seguridad Informática de la UPR, ver **(Anexo 12)** y la Vicerrectoria de Investigación y Postgrado, ver **(Anexo 13)**, por lo que el análisis es independiente para cada persona.

En la siguiente tabla presentaremos la Identificación Total de las amenazas, como resultado a las entrevistadas realizadas:

TABLA 3.IDENTIFICACION GENERAL DE AMENAZAS EN LA UPR.

No	AMENAZAS	Bienes Informáticos												
		1	2	3	4	5	6	7	8	9	10	11	12	13
1	Inundación		X	X	X		X			X				
2	Ciclones	X	X	X	X	X	X	X	X	X	X	X	X	X
3	Tormentas Eléctricas	X	X	X	X	X	X	X	X	X	X	X	X	X
4	Incendios	X	X	X	X	X	X	X	X	X	X	X	X	X
5	Robos	X	X	X	X	X	X	X	X	X	X	X	X	X
6	Fallas de Fluido Eléctrico	X	X	X	X	X	X	X	X	X	X	X	X	X
7	Falta de Control de ingreso de personas ajenas a las instalaciones	X	X	X	X	X	X	X	X	X	X	X	X	X
8	Alteración en el Software (S.O, Sistemas, herramientas)	X	X	X	X	X	X	X	X	X	X	X	X	X
9	Mal manejo del Software.	X	X	X	X	X	X	X	X	X	X	X	X	X
10	Destrucción o modificación de la Información	X	X	X	X	X	X	X	X	X	X	X	X	X
11	Carencia de respaldos periódicos de la Inform.(backups)	X	X	X	X	X	X	X	X	X	X	X	X	X
12	Falta de actualización de Bienes Informáticos	X	X	X	X	X	X	X	X	X	X	X	X	X
13	Manejo inadecuado de Estándares de redes	X	X	X	X	X	X	X	X	X	X	X	X	X
14	Contaminación de Virus Informáticos	X	X	X	X	X	X	X	X	X	X	X	X	X
15	Acceso de intrusos a la red	X	X	X	X	X	X	X	X	X	X	X	X	X
16	Diseminación de la Información no Autorizada a través de la RED	X	X	X	X	X	X	X	X	X	X	X	X	X
17	Climatización	X	X	X	X	X	X	X	X	X	X	X	X	X

A partir de las amenazas identificadas en la Tabla 3, se cuantifica el riesgo de que cada una de ellas se materialice sobre cada uno de los bienes informáticos.

3.13.2 ESTIMACIÓN DE RIESGOS SOBRE LOS BIENES INFORMÁTICOS EN LA UPR

A partir de las amenazas identificadas se cuantifica y estima el riesgo para cada bien informático, los valores numéricos para la asignación de riegos fue obtenida según detalla la metodología de la Institución, de forma numérica asignando valores entre cero y uno (0 sí la probabilidad de que se materialice la amenaza es nula y 1 sí es máxima).

Riesgo bajo	de 0 a 0,35
Riesgo medio	de 0,36 a 0,59
Riesgo alto	de 0,60 a 0,79
Riesgo muy alto	de 0,80 a 1

La estimación del riesgo sobre cada bien informático se determina a partir de las amenazas identificadas en la Tabla 3 y que actúan sobre cada uno de los bienes informáticos de la Institución.

A partir de esta valoración y de la importancia estimada (Wi) para cada bien informático en la tabla 2 de Evaluación de los bienes informáticos de la UPR, se puede determinar el peso del riesgo mediante la multiplicación de los valores obtenidos.

Peso = Ri * Wi

En donde:

- Las columnas 1 y 2 corresponden al Número de orden y Dominio y corresponden con las de la Tabla 2 Evaluación a los bienes informáticos de la UPR.
- Las columnas 3,……, 3n reflejan la probabilidad de que se materialicen las amenazas identificadas en la Tabla 3 sobre cada bien informático, asignando valores entre 0 y 1.
- La columna 4 es la valoración del riesgo sobre cada bien informático. Se calcula a partir del promedio de las columnas 3,……. 3n que tomaron valor, es decir, la suma de los valores de esas columnas entre la cantidad de columnas.
- La columna 5, corresponde a la Importancia del bien informático, se obtiene de los valores estimados en la columna 9 de la Tabla 2
- La columna 6, Peso del Riesgo sobre cada bien informático, se obtiene como resultado de la multiplicación de los valores de las columnas 4 y 5.

El Peso Relativo del Riesgo sobre cada bien informático se determina mediante la multiplicación del riesgo estimado (Ri) por la importancia relativa del bien informático (Wi/Wt). La suma de los Pesos Relativos de Riesgos sobre todos los bienes informáticos caracteriza el Peso Total del Riesgo del Sistema (Rt). De tal modo:

$$Rt = \sum_{i=1}^{n} Ri * Wi/Wt$$

Como:

$$Wt = W1 + W2 + ... + Wn = \sum_{i=1} Wi$$

Entonces:

$$Rt = \sum_{i=1}^{n} Ri * Wi \; / \sum_{i=1}^{n} Wi$$

Para presentar una estimación actual y significativa de los riesgos efectuamos entrevista a los grupos anteriormente mencionados:

Grupo de Redes y Diseño Web, ver (**Anexo 14).**

Dirección de Formación Científica, ver (**Anexo 15).**

Responsable de la Seguridad informática de la UPR, ver **(Anexo 16).**

Vicerrectoria de Investigación y Postgrado, ver **(Anexo 17)**.

A continuación se procederá a la Estimación de los Riesgos Totales de las amenazas que actúan los bienes informáticos de la UPR.

TABLA 4: ESTIMACIÓN TOTAL DE LOS RIESGOS SOBRE LOS BIENES INFORMÁTICOS DE LA UPR

Nº	DOM	AMENAZAS																	RIESGO Ri	IMPORT Wi	PESO Ri*Wi
		R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17			
1	D1	-	0,43	0,47	0,47	0,31	0,51	0,52	0,4	0,32	0,4	0,6	0,55	0,48	0,6	0,41	0,3	0,47	0,47	9,76	4,58
2	D2	0.2	0,48	0,6	0,36	0,51	0,57	0,52	0,53	0,37	0,7	0,76	0,6	0,58	0,71	0,52	0,52	0,55	0,53	8,37	4,43
3	D3	0,62	0,6	0,57	0,4	0,54	0,57	0,5	0,55	0,36	0,7	0,75	0,61	0,6	0,73	0,6	0,57	0,46	0,57	8,6	4,90
4	D4	0,3	0,54	0,64	0,43	0,48	0,52	0,52	0,53	0,38	0,7	0,72	0,6	0,7	0,76	0,55	0,62	0,57	0,56	8,30	4,64
5	D5	-	0,65	0,71	0,55	0,6	0,74	0,61	0,58	0,46	0,45	0,6	0,57	0,58	0,68	0,51	0,36	0,84	0,59	9,85	5,81
6	D6	0,5	0,45	0,4	0,38	0,28	0,42	0,66	0,61	0,56	0,43	0,61	0,4	0,56	0,64	0,61	0,51	0,36	0,49	8,07	3,95
7	D7	-	0,43	0,51	0,5	0,4	0,51	0,52	0,4	0,22	0,4	0,6	0,37	0,4	0,6	0,31	0,2	0,8	0,44	8,98	3,95
8	D8	-	0,66	0,57	0,55	0,58	0,7	0,72	0,53	0,44	0,6	0,76	0,48	0,3	0,7	0,58	0,36	0,43	0,56	7.02	3.93
9	D9	1	0,53	0,62	0,47	0,7	0,8	0,85	0,75	0,56	0,8	0,6	0,4	0,34	0,7	0,56	0,41	0,82	0,64	7,58	4,85
10	D10	-	0,43	0,51	0,4	0,46	0,51	0,52	0,4	0,4	0,4	0,6	0,5	0,4	0,55	0,3	0,2	0,82	0,43	8,80	3,78
11	D11	-	0,46	0.7	0,4	0,54	0,41	0,44	0,6	0,55	0,6	0,7	0,45	0,45	0,56	0,35	0,3	0,91	0,52	9.41	4,89
12	D12	-	0,4	0,33	0,36	0,43	0,53	1	0,55	0,6	0,55	0,6	0,5	0,3	0,6	0,3	0,3	0,7	0,50	5.21	2.60
13	D13	-	0,4	0,43	0,56	0,33	0,53	1	0,55	0,6	0,55	0,6	0,46	0,3	0,56	0,3	0,3	0,8	0,51	7.40	3.77
TOTAL																				**107.35**	**56.08**

Se pudo entonces, con los resultados obtenidos en la tabla 4, calcular y apreciar el Riesgo Total al que están expuestas las Tecnologías de la Información, en la Universidad de Pinar del Río, mediante la fórmula:

$$Rt = \sum_{i=1}^{n} Ri * Wi \; / \sum_{i=1}^{n} Wi$$

Analizando esta fórmula consideramos que:

Riesgo Total = Peso Total / Importancia Total

RT= 56,08 / 107,35

RT= 0,52

El valor obtenido, según la nueva propuesta metodología para el estudio de vulnerabilidad hace que la calificación del riesgo total en la **Universidad de Pinar del Rió,** sea de 0,52. Este número significa que existen el 52 por ciento de posibilidades a partir del 100 por ciento de que ocurra alguna de las amenazas reflejadas en la tablas 3.3 del informe, lo que expresa que la posibilidad de incidentes es real y requiere mucha atención.

3.14 RESULTADOS DEL ANÁLISIS DE RIESGOS

Quedan claramente definidos los siguientes aspectos:

- Qué bienes componen la infraestructura crítica del la Institución.
- Cuál es el grado de dependencia respecto a estos bienes informáticos.

- Qué amenazas actúan sobre ellos con mayor probabilidad y cuál sería su posible impacto.
- Qué amenazas están fuera del control de la Institución.
- A qué nivel de riesgo está sometido cada bien informático en la Institución.
- Detección temprana de los riesgos, como una respuesta oportuna y efectiva ante las pérdidas de posibles amenazas que pueden verse materializadas.

3.15 ESTRATEGIAS DE SEGURIDAD

Al desarrollar el Estudio de Vulnerabilidad en la **UPR** se considerará adecuado incorporar las siguientes Estrategias de Seguridad Informática, para tener un mejor control en cuanto a sus bienes.

- Mínimo privilegio

  Cualquier objeto (usuario, programa, sistema, etc.) debe tener solo los privilegios que necesita para cumplir la tarea asignada.

- Acceso

  El acceso a la información y sistemas será Cerrado (Todo aquello que no esté expresamente permitido está prohibido) y no Discrecional (La decisión sobre lo que se puede hacer no corresponde a su creador o dueño sino a la Dirección).

- Defensa en profundidad

  La defensa no debe estar basada en un solo mecanismo de seguridad por muy fuerte que este parezca. Por el contrario, deben habilitarse múltiples mecanismos que se respalden unos a otros.

- Diversidad de la defensa

  Utilización de diferentes tipos sistemas para reducir la posibilidad de explotación malintencionada de errores conocidos y para limitar el alcance de un ataque.

- Punto de choque

  Un canal único de entrada que pueda ser monitoreado y controlado. Un punto de choque es inútil si existen otras vías por las que un intruso pueda penetrar al sistema.

- Eslabón más débil

  Un sistema es tan fuerte como su parte más débil. Un atacante, como regla, primero analiza cuál es el punto más débil del sistema y concentra sus esfuerzos en ese lugar.

- Proporcionalidad

  Las medidas de seguridad deben estar en correspondencia con la importancia de lo que se protege y con el nivel de riesgo existente.

- Participación universal

  Es necesario contar con una participación activa del personal interno en interés de apoyar el sistema de seguridad establecido.

- Uso del sentido común

  De nada valen mecanismos de defensa muy sofisticados si se violan las normas más elementales.

3.16 ANÁLSIS DE POLÍTICAS DE SEGURIDAD EN LA UPR

El propósito de las políticas de seguridad informática es proteger la información y los bienes informáticos de la UPR, las políticas son guías para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación, redes e instalaciones de cómputo.

Para evaluar el cumplimiento que se da a las políticas de seguridad informática implantas en la UPR con respecto a la tecnología y recursos informáticos que utiliza la Institución, se dirigió una encuesta, ver **(Anexo 18)** a determinados grupos de personas que forman parte de la comunidad universitaria, entre ellos tenemos:

- Estudiantes
- Trabajadores Docentes
- Trabajadores no Docentes
- Administrativos o Administradores

El resultado obtenido de este análisis, ver **(Anexo 19)** nos permite proponer el rediseño algunas de las políticas de seguridad Informática que actualmente se encuentran en vigencia dentro de la Institución, ver **(Anexo 20)**, siendo su selección y rediseño producto del resultado obtenido en el análisis de riesgos y vulnerabilidades aplicado a los bienes informáticos de la UPR.

- Los usuarios (Los estudiantes, docentes y trabajadores) de las diferentes áreas son responsables de la protección de la información que utilicen o creen en el transcurso del desarrollo de sus labores por ello se deben implementar medidas de seguridad física para asegurar la integridad de las instalaciones y laboratorios de cómputo. Las medidas de protección deben ser consistentes con el nivel de clasificación de los bienes y el valor de la información procesada y almacenada en las instalaciones.

- Se realizará un inventario del software instalado en los laboratorios y en cada uno de los departamentos de la Universidad, ya sea con respecto al código fuente, programas de uso general y el tratamiento que requiere la información

oficial que se procese, intercambie, reproduzca o conserve a través de las tecnologías de información, según su categoría y demás regulaciones.

- Cualquier violación que se detecte en materia de seguridad informática, es obligatorio comunicársela al Responsable de Seguridad quien tratará de remediar lo ocurrido, reportado el incidente de seguridad, éste debe ser investigado por el Responsable en cual debe identificar la severidad del incidente para la toma de medidas correctivas, manteniendo una documentación de todos los incidentes ocurridos en la UPR.

- Se realizarán periódicamente auditorías internas a cada actividad donde se involucren aspectos de seguridad lógica y física estableciendo un calendario dirigido a cada área, en el cual se evaluará el estado actual de funcionamiento de los bienes informáticos para tener mejor auditabilidad de los sistemas instalados y a su vez poder reportar información para la gestión de riesgos de la UPR.

- Específicamente los estudiantes de la **UPR** tendrán acceso y harán uso de las tecnologías de la información de acuerdo con sus planes de estudio, pero la información “Confidencial o “Restringida” debe ser asegurada para que esté solo disponible a los individuos específicamente autorizados para acceder a ella, el ambiente donde se almacena la información clasificada como “Restringida”, debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia.

- El programa antivirus debe encontrarse habilitado en todos los equipos de computo de la Institución y debe ser actualizado periódicamente, sea manual o automáticamente, en el caso de detectar fallas en el funcionamiento de dichos

programas estas deben ser comunicadas al responsable de seguridad informática.

- Ante una infección de virus, se informará al Responsable de Seguridad Informática el mismo que deberá realizar esfuerzos necesarios para determinar el origen de la infección y evitar la reinfección de los demás equipos de cómputo en la Institución

- Todas las contraseñas deben tener una longitud mínima de ocho (8) caracteres y no deben contener espacios en blanco, éstas deben ser difíciles de adivinar. Las contraseñas deben contener al menos un carácter alfabético en mayúscula y uno en minúscula.

- El usuario y los administradores serán los responsables de mantener y controlar el espacio libre en las cuenta de correo para permitir la correcta recepción de los mensajes. Se aconseja revisar la cuenta diariamente.

3.17 DISEÑO DE NUEVAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

Como un aporte significativo del grupo investigador proponemos el diseño de las siguientes políticas de seguridad informática, las mismas que fueron elaboradas en base a las encuestas realizadas y bajo las regulaciones y leyes a las que la Institución se haya sujeta, también se analizó la información necesaria de la norma **UNE-ISO/IEC 17799**, que compete a la gestión de riesgos e irán enmarcadas a contribuir y a mantener la integridad, confidencialidad y disponibilidad de los recursos de la Institución.

- Elaborar programas de educación continua para los estudiantes, docentes y empleados, en temas relacionados a la Seguridad informática, en coordinación con cada una de las Facultades de la Universidad.

- Se diseñarán manuales de funciones para definir y evaluar una estructura jerárquica adecuada y lograr un mejor desempeño en cada una de las tareas a nivel de administradores y personal encargado de utilizar los sistemas, datos, redes e información de la Institución.

- Los bienes de la institución que sean de propósito específico y tenga una misión crítica asignada, requiere ser reubicado en áreas que cumplan con los requerimientos de: Seguridad física, las condiciones ambientales y la alimentación eléctrica adecuada.

- A los Administradores le corresponderá la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar, para este fin debe emitir las normas y procedimientos respectivos.

- Corresponde al Grupo de Redes de la UPR, dar a conocer las listas de las personas, que puedan tener acceso físico a los locales donde se encuentran alojados los bienes informáticos considerados como críticos dentro de la Institución y se llevará un registro permanente del ingreso del personal a las Instalaciones.

- Los administradores de las redes serán las personas encargadas de difundir el reglamento para el uso de la red y de procurar su cumplimiento.

- Se realizará un diagnostico por Facultad sobre la necesidad del software de ser instalado en cada uno de los laboratorios y departamentos de la UPR.

- Será tarea del responsable de seguridad informática promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información. Realizar un programa de concientización en seguridad a través de continuas capacitaciones y charlas, adicionalmente se pueden emplear diversos métodos como afiches, mensajes de mail, etc; los cuales recuerden permanentemente al usuario el papel importante que cumplen en el mantenimiento de la seguridad de la información.

- El personal encargado de la seguridad informática debe ser plenamente identificado por todos los estudiantes, docentes y empleados de la UPR, a fin de ser fácilmente ubicado en cualquier momento.

- Los administradores de los recursos realizarán pruebas trimestrales sobre la calidad de las contraseñas que son empleadas por los usuarios, para determinar su nivel de seguridad.

- Todos los bienes y sistemas que procesan información deben estar aislados físicamente de áreas críticas como inundaciones e incendios, etc.

- El responsable de seguridad Informática verificará el cumplimiento de las políticas implantadas y evaluará continuamente cualquier cambio con relación a los riesgos físicos.

- El plan de seguridad Informática, debe ser difundido y publicado con su debida actualización a través de varios medios de comunicación, para que su alcance sea a nivel general de la Institución.