ANÁLISIS DE RIESGO

[Nombre de la Institución]

[FECHA]

[NOMBRE DE LA COMPAÑÍA]

[Dirección de la compañía]

ANÁLISIS DE RIESGO

REV. ___	Nombre y Apellidos	Cargo	Fecha	Firma
Confeccionado				
Aprobado.				
Revisado.				

PAGINAS REVISADAS:

REV. ___	ELABORADO	REVISADO	APROBADO
NOMBRE			
CARGO			
FIRMA			
FECHA			

Tabla de Contenido

1. Introducción

[Breve introducción sobre el Sistema Informático de la Entidad]

2. Objetivos del estudio de vulnerabilidad

[Ejemplos de objetivos:

- ✓ ***Determinar los sistemas críticos para la gestión de cada Organismo, en particular los soportados en redes de datos, las amenazas que actúan sobre ellos, los niveles de riesgo y el posible impacto.***
- ✓ ***Determinar el grado de dependencia actual y perspectivo con relación a estos sistemas.***
- ✓ ***Establecer las políticas que se requieran para minimizar los riesgos sobre los bienes informáticos críticos e implementar las acciones y mecanismos que se necesiten para su prevención, detección y recuperación.***
- ✓ ***Determinar los parámetros que permitan establecer niveles mínimos de disponibilidad permisibles.***
- ✓ ***Establecer un sistema que garantice la continuidad de este estudio sobre la base de los cambios que surjan y los incidentes que se produzcan.***

]

3. Alcance

[Se considerarán en el estudio:

- ✓ ***Redes de diferentes tipos***
- ✓ ***Intranet***
- ✓ ***Extranet***
- ✓ ***Internet***
- ✓ ***Otros tipos de redes de importancia***
- ✓ ***Sistemas automatizados de control de proceso.***
- ✓ ***Sistemas de gestión de datos de interés institucional.***
- ✓ ***Aplicaciones de gran importancia para el funcionamiento del Organismo.***

]

4. Definiciones

[Amenaza, situación o acontecimiento que pueda causar daños a los bienes informáticos.

Riesgo, probabilidad de que se produzca un daño.

Impacto, daños producidos por la materialización de una amenaza.

Vulnerabilidad, califica el nivel de riesgo de un sistema.

Sistemas críticos, aquellos cuya afectación puede paralizar o afectar severamente la gestión de una organización.

Incluir otras definiciones que sean de interés de la institución

]

5. Etapas de realización del estudio de vulnerabilidad.

[

1. ***Determinar cuáles son las necesidades de protección de los sistemas objeto de análisis.***
2. ***Definir las acciones que garanticen minimizar los riesgos identificados en la primera etapa.***
3. ***Evaluación de las soluciones diseñadas.***

]

5.1 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.

En resumen, durante la determinación de las necesidades de protección de los sistemas informáticos es necesario:

a) ***Caracterizar el entorno informático.***
b) ***Identificar las amenazas potenciales sobre los sistemas informáticos y estimar los riesgos sobre los mismos.***

c) Evaluar el estado actual de la seguridad.

]

5.1.1 Caracterización del entorno informático.

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

- ✓ *Tecnologías utilizadas y su organización.*
- ✓ *Redes instaladas, estructura, tipo y plataformas que utilizan.*
- ✓ *Sistemas en explotación y servicios disponibles.*
- ✓ *Características del procesamiento, transmisión y conservación de la información, teniendo en cuenta los flujos interno y externo y los niveles de clasificación de la misma.*
- ✓ *Otros datos de interés.*

Dada las características de este trabajo a nivel de Organismo, no es necesario incluir la totalidad de los bienes informáticos, pudiendo no tenerse en cuenta aquellos cuyo peso relativo sea obviamente poco significativo. De igual modo para sistemas, tecnologías o servicios iguales en entidades del mismo tipo y sometidos a amenazas similares puede realizarse el estudio sobre uno y generalizarse a los demás, aunque lo ideal sería que cada entidad lo realizara de forma independiente, comparando posteriormente los resultados.

Una vez identificados los bienes informáticos que necesitan ser protegidos es necesario determinar su importancia dentro del sistema informático y clasificarlos según la misma.

La valoración de los bienes informáticos posibilita, mediante su categorización, determinar en qué medida uno es más importante que otro y se realiza teniendo en cuenta aspectos tales como la función que realizan, su costo, la repercusión que ocasionaría la pérdida del mismo, así como la confidencialidad, la integridad y la disponibilidad.

La determinación de la importancia de los bienes informáticos puede ser realizada de forma descriptiva (por ejemplo, valor alto, medio, bajo) o de forma numérica asignando valores entre cero y diez (0 si no tiene importancia y 10 sí es máxima). La 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. Una posible relación entre los métodos descriptivos y numéricos podría ser:

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

Las Tablas 1 y 2 muestran una forma de relacionar los bienes informáticos que forman parte del sistema, valorando su importancia a partir del papel que juegan dentro del mismo. En el caso de bienes informáticos similares, destinados a cumplir funciones análogas y sometidas a las mismas amenazas, no es necesario repetirlos en la relación que se haga, pues las estimaciones que se realicen para uno, serán similares en los demás.]

TABLA 1 **IDENTIFICACION DE BIENES INFORMATICOS**

No	DESCRIPCION	TIPO	UBICACIÓN
1	2	3	4

Donde 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 tipos***

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.

TABLA 2 **EVALUACION DE BIENES INFORMÁTICOS**

		VALORACION POR ASPECTOS	IMPORT

No	DOM	FUNC	COSTO	IMAGEN	CONFID.	INTEG.	DISPON.	. (Wi)
1	2	3	4	5	6	7	8	9

En cada una de las filas de esta tabla se relacionan los bienes informáticos identificados en la tabla 1 a fin de facilitar la evaluación de cada uno de ellos. El significado de cada una de las columnas es el siguiente:
NUMERO de orden consecutivo (se obtiene de la TABLA 1)
DOMINIO: Identificación para agrupar bienes informáticos afines por las funciones que realizan y/o por la administración sobre ellos. (D1,D2,...,Dn, según la cantidad que se cree).
FUNCION: Importancia de la tarea que cumplen los bienes informáticos.
COSTO: Valor y valor de uso de los bienes informáticos.
IMAGEN: Repercusión interna y/o externa que ocasionaría la pérdida de los bienes informáticos.
CONFIDENCIALIDAD: Necesidad de proteger la información que de los bienes informáticos pueda obtener.
INTEGRIDAD: Necesidad de que la información no se modifique o destruya.
DISPONIBILIDAD: Que los servicios que de bienes informáticos se esperan puedan ser obtenidos en todo momento de forma autorizada.
IMPORT. (Wi): Importancia de los bienes informáticos.
Al estimar la repercusión que ocasionaría la pérdida de los bienes informáticos se debe tener en cuenta el tiempo que la entidad puede seguir trabajando sin los mismos, lo que puede ser vital para su funcionamiento. Este tiempo puede oscilar entre escasas horas hasta días y semanas. Esto puede depender también del ciclo de utilización del mismo.
A las columnas de la 3 a la 8 se le asignan valores entre 0 y 10, a partir de la estimación que se haga de la importancia de cada uno de estos factores sobre los bienes informáticos analizados (0 sino tiene importancia y 10 si es máxima).
La columna 9 (Wi) cuantifica la importancia de los bienes informáticos y se calcula por el promedio de los valores de la 3 a la 8, es decir, el resultado de la suma de éstas dividido por 6. La suma total (Wt) de los valores (Wi) obtenidos en la columna 9 representa la importancia total de los bienes informáticos que componen el sistema:

Wt = W1 + W2 + ... + Wn

Bienes informáticos críticos.

Como resultado de la evaluación anterior se deben determinar los bienes informáticos que se consideran críticos para el Organismo. Se consideran bienes informáticos críticos aquellos sin los cuales el trabajo no puede ser ejecutado o fuera afectado de forma sensible.
Los bienes informáticos críticos tienen carácter relativo según la entidad de que se trate, por ejemplo, la destrucción o modificación de una base de datos en un Organismo de la Administración Central del Estado posiblemente no tenga la misma connotación que si ocurre en una empresa de producción y servicios.
En la columna No. 9 de la tabla No 2, se determinaron los niveles de importancia de los bienes informáticos. Esta tarea no se debe limitar solo a los cálculos anteriormente realizados. Un cálculo pudiera dar como resultado que un sistema cualquiera no tiene significación alguna para una entidad, pero la práctica pudiera indicar otra cosa. Todo no se le puede confiar a un simple cálculo aritmético.
Lo anterior implica un análisis complementario de los datos obtenidos de la Tabla No. 2, que podría realizarse de la forma siguiente:

- ***Señale adecuadamente aquellos bienes informáticos que fueron valorados de importancia significativa.***
- ***Señale aquellos bienes informáticos, que no habiendo sido valorados de importancia significativa, tienen una incidencia directa con algún otro crítico.***
- ***Señale, después de un estudio riguroso y detallado, aquellos bienes informáticos que no teniendo una valoración significativa, ni incidencia directa en el trabajo de activos y recursos críticos, resulta necesario que sean marcados como tales, por razones prácticas.***
- ***Actualice la tabla No.2 a partir de las consideraciones anteriores.***

5.1.2. 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 éstos y estimar la pérdida potencial (impacto) que puede producir su materialización.

Por su origen las amenazas se clasifican en accidentales e intencionales, a partir de que su ocurrencia sea premeditada o no. Las amenazas accidentales pueden ser originadas por causas naturales o por causas laborales o sociales.

Las amenazas intencionales implican la voluntad o intención de materializarlas.

Una amenaza intencional, si se materializa se considera una agresión o ataque. Las amenazas intencionales (ataques) pueden ser internas o externas. Un ataque interno ocurre cuando usuarios legítimos de un sistema se conducen de forma no autorizada. Los métodos de protección que pueden ser usados contra ataques internos incluyen:

- ***Selección cuidadosa del personal.***
- ***Supervisión del hardware, el software, las políticas de seguridad y la configuración de los sistemas, de modo que haya un grado de seguridad de que funcionen correctamente.***
- ***Empleo de las trazas de auditoría para incrementar la probabilidad de detección de tales ataques.***

Los ataque externos se producen por lo general mediante el empleo de las posibilidades de acceso remoto para el uso de usuarios autorizados y pueden emplear técnicas tales como las siguientes:

- ***Suplantación de usuarios del sistema o sus componentes.***
- ***Eludir mecanismos de autenticación o de control de acceso.***
- ***Intervención de líneas.***
- ***Intersección de emisiones.***

Por sus efectos o consecuencias las amenazas se clasifican en pasivas y activas. Las amenazas pasivas son aquellas que de materializarse no implican ninguna modificación a la información contenida en el sistema ni cambios en el estado del mismo, por ejemplo fuga de información. Las amenazas activas implican la alteración de la información contenida en el sistema o cambios en el estado del mismo, por ejemplo modificación no autorizada de una base de datos.

Para cada bien informático a proteger los objetivos fundamentales de seguridad son la confidencialidad, la integridad y la disponibilidad, por lo que hay que determinar cada amenaza sobre la base de como pueda afectar a estas características. Por supuesto, el peso que cada una de estas características tiene para los activos o recursos varía de una entidad a otra, en dependencia de la naturaleza de los procesos informáticos que se llevan a cabo en función del objeto social de cada entidad. Algunas de las amenazas más comunes son las siguientes:

- ***Destrucción de información.***
- ***Corrupción o modificación de información.***
- ***Hurto, traslado o pérdida de activos y/o recursos.***
- ***Divulgación de información.***
- ***Interrupción de servicios.***

La realización de un análisis de riesgos implica el examen de cada una de las amenazas sobre los bienes informáticos y su clasificación por niveles, a partir de la probabilidad de su ocurrencia y la severidad del impacto que puedan producir.

A partir de las amenazas identificadas se cuantifica el riesgo de que cada una de ellas se materialice sobre cada uno de los bienes informáticos, ésto puede ser realizado de forma descriptiva (por ejemplo, riesgo alto, medio, bajo) o 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). Al igual que para la Tabla No. 2 una posible relación entre los métodos descriptivos y numéricos podría ser:

- ***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 1,0***

La estimación del riesgo sobre cada bien informático se determina a partir de las probabilidades de materialización estimadas de las diferentes amenazas que actúan sobre el mismo. A partir de esta valoración y de la importancia estimada para cada bien informático (ver 2.1.) se puede determinar el peso del riesgo (mediante la multiplicación de los valores obtenidos, en el caso de haberlos estimado de forma numérica).

La Tabla 3 permite la realización de un análisis cruzado a partir de la identificación de las amenazas que pueden actuar sobre el sistema informático y su incidencia sobre cada uno de los bienes informáticos que componen el mismo. En cada una de las filas de esta tabla se relacionan las amenazas, numerándolas consecutivamente para su posterior identificación en la Tabla 4. Se abrirá una columna para cada bien informático identificado en la Tabla 1, marcando con una cruz en la fila correspondiente a cada amenaza que incida sobre él.]

IDENTIFICACION DE AMENAZAS

TABLA 3

No.	AMENAZAS	BIENES INFORMATICOS				
		1 N			2 3	
1						
2						
.						
.						
M						

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, con ayuda de la Tabla 4.

ESTIMACION DE RIESGOS SOBRE LOS BIENES INFORMATICOS

TABLA 4

No	DOM	AMENAZAS				Riesgo Ri	Import. Wi	Peso Ri * Wi
		R1	R2	R3	..... Rn			

1	2	3	31	32	..... 3n	4	5	6
1								
2								
. . .								
N								

- ***Las columnas 1 y 2 (Número de orden y Dominio) corresponden con las de la Tabla 2.***
- ***Las columnas 3, 31, 32, ..., 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, 31, 32, ..., 3n que tomaron valor, es decir, la suma de los valores de esas columnas entre la cantidad de columnas.***
- ***La columna 5, 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:

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

Entonces:

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

De manera que el Peso Total del Riesgo del Sistema (Rt) se puede obtener dividiendo la suma total de los valores de la columna 6 (Ri * Wi) por los de la columna 5 (Wi). De forma análoga se puede determinar el riesgo sobre un dominio dado.
Por este procedimiento se puede estimar el peso del riesgo para un grupo de elementos, un área o el sistema completo.
El método explicado brinda la posibilidad de conocer que bien informático, o que área en particular está sometida a un riesgo mayor y de que naturaleza, lo que permite la selección adecuada de los mecanismos de seguridad que deben ser establecidos en cada uno de los casos, garantizándose de esta manera una correcta proporcionalidad por medio de una buena relación entre costos y beneficios.

5.1.3. Evaluación del estado actual de la seguridad.

[Generalmente las entidades que emplean las tecnologías de la información en el desarrollo de su actividad, aunque no hayan diseñado un sistema de seguridad informática que considere de forma integral todos los factores que deben tenerse en cuenta, tienen implementadas determinadas normas, medidas y procedimientos de seguridad, casi siempre de forma empírica a partir de incidentes que han ocurrido o de las experiencias de otras entidades, lo cual por supuesto es insuficiente y da lugar a la existencia de vulnerabilidades.

Considerando lo anterior, el siguiente paso en esta primera etapa consiste en evaluar de manera crítica la efectividad de las políticas y controles de seguridad existentes, sobre la base de los resultados del análisis de riesgos realizado, con el objetivo de perfeccionarlas o sustituirlas por aquellas que brinden la respuesta adecuada.]

5.1.4. Resultados del análisis de riesgos.

Antes de pasar a la segunda etapa deben haber quedado claramente definidos los siguientes aspectos:

- ***Que elementos componen la infraestructura crítica del Organismo.***

- ***Cuál es el grado de dependencia respecto a estos elementos.***
- ***Que amenazas actúan sobre ellos con mayor probabilidad y cuál sería su posible impacto.***
- ***Interdependencia con otros sistemas (internos y externos).***
- ***Como afectaría al país y su posible impacto internacional.***
- ***Que amenazas están fuera del control del Organismo.***
- ***Cuál es la mejor manera de prevenir, minimizar y manejar los riesgos.***
- ***Parámetros que permitan establecer niveles mínimos de disponibilidad permisibles.***