METODOLOGIA
PARA LA REALIZACION DEL ESTUDIO DE VULNERABILIDAD DE LOS SISTEMAS INFORMATICOS

Í

1. Introducción

A pesar del incipiente desarrollo que aun tiene nuestro país en el empleo a gran escala de las tecnologías de la información, la realidad nos indica que se presentan en nuestro caso las mismas amenazas y características que se refieren en toda la literatura sobre el tema en países con mucha mayor experiencia, tanto en los objetivos e impacto de los ataques a redes, 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 nuestra condición de país agredido por poderosos e inescrupulosos enemigos. Importantes amenazas se concentran en actos de espionaje político, militar y económico; el vandalismo, la destrucción de datos, tráfico de drogas, juego prohibido, control de las redes de forma remota y otros.

La naturaleza propia de las redes de datos, en especial la extensión de su radio de acción, implica que el impacto de un problema de seguridad, ya sea accidental o intencional, rebase por lo general, los limites de una entidad u organización en particular, pudiendo alcanzar una repercusión que comprometa a toda la sociedad.

En Cuba, a pesar de que aún no se ha logrado ni remotamente 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 la vulnerabilidad de nuestros sistemas informáticos, todos los cuales sin excepción están expuestos a las más variadas y comprometidas amenazas.

Consecuentemente con el resultado del estudio de la vulnerabilidad es preciso emprender los esfuerzos necesarios para en una primera etapa de forma expedita corregir las debilidades que se detecten en los sectores claves, a la par que se proyecte una organización de alcance estratégico que involucre todas las instituciones gubernamentales, docentes, científicas, productivas, militares y de seguridad.

Debido a lo anterior resulta imprescindible desarrollar una estrategia a largo plazo para tratar estos problemas, determinando los elementos más sensibles a verse interrumpidos dentro del proceso de informatización que se viene produciendo.

Esta estrategia debe ser 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. La misma además, debe considerar la creación de un mecanismo de cooperación entre las distintas redes, que respalde y coordine los esfuerzos entre las mismas, al tiempo que identifique y generalice las mejores experiencia en este sentido.

2. Objetivos del estudio de vulnerabilidad

- ✓ 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. Cuestiones básicas

Durante la preparación y realización del estudio deberán determinarse:

- ♦ ¿Qué escenarios deben ser considerados? o sea, que sectores o áreas sustentan su actividad en redes, sistemas o aplicaciones considerados como críticos.
- ♦ ¿Cuáles son los riesgos y que amenazas los provocan?
- ♦ ¿Qué impacto podría esperarse?
- ♦ ¿Cómo manejar los riesgos?

5. 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.

6. Etapas de realización del estudio de vulnerabilidad.

1) Determinar cuales 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.

6.1. 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 el proceso de análisis de riesgos se pueden diferenciar dos aspectos:

1) La **Evaluación de Riesgos**, orientada a determinar los sistemas que, en su conjunto o en cualquiera de sus partes, pueden verse afectados directa o indirectamente por amenazas, valorando todos los riesgos y estableciendo sus distintos niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la entidad.
2) La **Gestión de Riesgos**, que implica la identificación, selección, aprobación y manejo de los controles a establecer para eliminar o reducir los riesgos evaluados a niveles aceptables, con acciones tendientes a:
    - Reducir la probabilidad de que una amenaza ocurra.
    - Limitar el impacto de una amenaza, si esta se manifiesta.
    - Reducir o eliminar una vulnerabilidad existente.
    - Permitir la recuperación del impacto o su transferencia a terceros.

Un primer análisis de riesgos será mucho más costoso que los sucesivos. Puede requerir mucho tiempo y la participación de personal especializado, lo cual estará en proporción a los objetivos planteados y su alcance.

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 los anterior, es necesario actualizar sistemáticamente el análisis de riesgos, utilizando como punto de partida el último realizado y los controles ya implementados, lo que posibilitará que el tiempo y los medios necesarios para su realización sean menores.

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.

6.1.1. 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 que 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 sometidos 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

No	DOM	VALORACION POR ASPECTOS						IMPORT. (Wi)
		FUNC	COSTO	IMAGEN	CONFID.	INTEG.	DISPON.	
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:

1. NUMERO de orden consecutivo (se obtiene de la TABLA 1)
2. 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).
3. FUNCION: Importancia de la tarea que cumplen los bienes informáticos.
4. COSTO: Valor y valor de uso de los bienes informáticos.
5. IMAGEN: Repercusión interna y/o externa que ocasionaría 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.

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.

Puede que un recurso sea muy costoso y por ello considerado de importancia alta, y sin embargo no es imprescindible para la gestión de la entidad. Estas circunstancias pueden elevar de forma artificial el nivel de importancia con que ha sido catalogado.

Un aspecto de vital importancia es la concatenación, o sea, la dependencia entre los bienes informáticos. En la práctica se da el caso que un activo o recurso resulta no ser importante tratado individualmente, para el correcto funcionamiento de una tarea cualquiera, pero, como elemento de un sistema, es el preámbulo o

paso anterior obligado para el funcionamiento de otro activo o recurso que ha sido marcado como importante. En este caso todos los bienes informáticos que cumplen con esa condición han de ser considerados como importantes.

Las comisiones que se creen deben velar porque las distintas estructuras que conforman un Organismo no declaren importantes aquellos activos o recursos que en realidad no lo son. Esto evitaría gastos innecesarios. Los cuadros administrativos, por lo general, tienden a declarar como importantes (críticos) a activos y recursos que en realidad no lo son.

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.

6.1.2. 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 esta 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.

Como se puede apreciar, el método explicado brinda la posibilidad de precisar de una manera exhaustiva los niveles de riesgos a que está sometido el sistema en cada una de sus partes componentes, a partir de lo cual se pueden determinar con racionalidad los controles de seguridad que deben ser implementados. La profundidad con que el mismo sea aplicado determinará la calidad del sistema diseñado.

La aplicación de los elementos aquí expuestos puede ser realizada con mayor o menor rigor, en dependencia de la composición y del nivel de preparación del equipo de trabajo designado para acometer esta tarea y de la participación que se dé a otras personas, que sin formar parte del equipo, puedan brindar los elementos que se requieran.

Por otra parte, desde el momento que los resultados dependen de valores estimados, las conclusiones a que se arribe deben ser tomadas como una aproximación al problema, que puede ser ajustada en sucesivas versiones, en correspondencia con la práctica diaria. Lo importante, en última instancia, es realizar el análisis de riesgos. Los conceptos anteriormente explicados pueden ser aplicados en diversas variantes y con más o menos rigor, pero de alguna forma es imprescindible empezar a utilizarlos.

A continuación se muestra un ejemplo práctico de la determinación de las necesidades de protección en un Organismo mediante la identificación y evaluación de los bienes informáticos a proteger, la determinación de las amenazas que actúan sobre ellos y la estimación de los riesgos:

Supongamos que un Organismo cuenta con una intranet para el intercambio de información entre sus entidades, un sistema general de contabilidad y un sistema automatizado de control de procesos industriales.

TABLA 1

IDENTIFICACION DE BIENES INFORMATICOS

No	DESCRIPCION	TIPO	UBICACIÓN
1	Intranet	RD	Todo el Organismo
2	Sistema general de contabilidad	GD	Areas económicas
3	Sistema de control de procesos industriales	CP	Area industrial

TABLA 2

EVALUACION DE BIENES INFORMATICOS

No	DOM	VALORACION POR ASPECTOS						IMPORT. (Wi)
		FUNC	COSTO	IMAGEN	CONFID.	INTEG.	DISPON.	
1	D1	7,0	8,0	7,0	9,0	7,0	7,0	7,5
2	D2	8,0	6,0	9,0	8,0	9,0	8,0	8,0
3	D3	8,0	8,0	9,0	8,0	9,0	9,0	8,5

TABLA 3

AMENAZAS CONTRA BIENES INFORMATICOS

No.	**BIENES INFORMATICOS** **AMENAZAS**	1	2	3
1	Acceso no autorizado	x	x	x
2	Modificación de información	x	x	x
3	Contaminación por virus	x	x	
4	Fuga de información	x	x	x
5	Fallo de software	x	x	x
6	Fallo de hardware	x	x	x
7	Fallo de energía eléctrica	x	x	x
8	Error de operación	x	x	x
9	Robo o hurto parcial o total	x	x	x
10	Deterioro físico	x	x	x
11	Alteración de la configuración	x	x	x
12	Modificación de los controles de seguridad	x	x	x

TABLA 4

ESTIMACION DE RIESGOS SOBRE LOS BIENES INFORMATICOS

BI	Dom	AMENAZAS												Riesgo Ri	Import.Wi	Peso Ri*Wi
		R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12			
1	D1	0,9	0,9	0,9	0,9	0,7	0,6	0,7	0,5	0,8	0,6	0,8	0,7	0,75	7,5	5,62
2	D2	0,8	0,9	0,7	0,8	0,7	0,6	0,6	0,6	0,5	0,6	0,6	0,7	0,67	8,0	5,36
3	D3	0,6	0,6		0,7	0,6	0,8	0,8	0,6	0,5	0,7	0,5	0,6	0,64	8,5	5,44
TOTALES:															24,0	16,42

El Peso Total del Riesgo en el ejemplo anterior se obtiene como resultado de dividir los totales de las dos últimas columnas de la Tabla No. 4, o sea:

Rt = 16,42 / 24,0 = 0,68 (Peso de Riesgo alto)

De los resultados obtenidos se infiere que debe ser definido un grupo de políticas que consideren, entre otros, los siguientes aspectos:

- La necesidad de limitar las posibilidades de accesos no autorizados a la intranet y al sistema general de contabilidad.
- El establecimiento de controles de auditoría sobre las acciones que se realicen en el sistema.
- La implantación de regulaciones relacionadas para la protección contra virus informáticos.
- Lo relacionado con la garantía de la continuidad de los procesos ante fallos de SW, HW o energía eléctrica.
- La preparación del personal.
- La protección física de los equipos y soportes magnéticos.
- La cantidad de copias (salvas de datos y programas) que deben realizarse y su lugar de conservación.
- La protección de los controles de seguridad que se establezcan.

A partir de estas políticas se debe establecer las medidas específicas dirigidas a obstaculizar las amenazas identificadas sobre cada bien informático en particular, a partir de su probabilidad de ocurrencia y el peso de riesgo estimado para cada uno de ellos, disminuyendo de esta forma el peso total del riesgo. El mayor interés recaería por supuesto en las amenazas más probables.

6.1.3. 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.

6.1.4. 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.
- Cual es el grado de dependencia respecto a estos elementos.
- Que amenazas actúan sobre ellos con mayor probabilidad y cual 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.
- Cual es la mejor manera de prevenir, minimizar y manejar los riesgos.
- Parámetros que permitan establecer niveles mínimos de disponibilidad permisibles.

6.2. Segunda etapa.- Definición e implementación de las acciones que garanticen minimizar los riesgos.

Una vez que se ha determinado qué debe ser protegido y estimados los riesgos sobre los bienes informáticos es necesario definir las políticas de seguridad que deben regir el funcionamiento de los sistemas y las acciones que hay que implementar para garantizar el cumplimiento de estas políticas.

Algunas de las interrogantes que deben ser resueltas al diseñar una política de seguridad son las siguientes:

1. ¿A quién se le permite utilizar los bienes informáticos?
2. ¿ Cuál es el uso correcto de los recursos?
3. ¿Quién está autorizado para garantizar el acceso y aprobar el uso de los sistemas?
4. ¿ Quién debe tener privilegios de administración de los sistemas?
5. ¿Cuáles son los derechos y responsabilidades de los usuarios?
6. ¿Cuáles son los derechos y responsabilidades de los administradores de los sistemas frente a los de los usuarios?

Por supuesto que estas no son las únicas interrogantes que deben ser resueltas en el diseño de una política. En la práctica surgen otras no menos importante.

Características de una buena política.

Las principales características que debe tener una buena política de seguridad son:

- Debe poder implementarse a través de procedimientos de administración de sistemas, la publicación de principios de uso aceptable u otros métodos apropiados.

- Debe poder hacerse cumplir por medio de herramientas de seguridad, donde sea apropiado y con sanciones, donde su prevención no sea técnicamente posible.

- Debe definir claramente las áreas de responsabilidad de los usuarios, administradores y dirigentes.

Criterios a considerar

- Hay que tener en cuenta el objeto social del Organismo y sus características. Por ejemplo la seguridad de una entidad comercial es muy diferente a la de un organismo central o a la de una universidad.

- Las políticas de seguridad que se desarrollen deben corresponder a las políticas, reglas, regulaciones y leyes a la que el Organismo está sujeto.

- A menos que el sistema informático a proteger esté completamente aislado e independiente, es necesario considerar las implicaciones de seguridad en un contexto más amplio. Las políticas deben manejar los asuntos derivados de un problema de seguridad que tiene lugar por causa de un sitio remoto, así como cuando ocurre un problema en un sitio remoto como resultado de un usuario o computadora local.

6.2.1. Estrategias de Seguridad

- **Mínimo privilegio**

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

- **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 cual 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.

6.2.2. Controles de Seguridad

Las acciones que se implementen deben corresponder con las políticas definidas y representan la línea de defensa básica de los sistemas objeto de protección, por lo cual es muy necesario seleccionarlas correctamente, de forma que cubran las amenazas identificadas, implementándolas de una manera rentable.

Tipos de acciones a considerar:

- Preventivas
- Detectivas
- Correctivas o de recuperación

Los controles de seguridad se implementan mediante la combinación de:

- Medios técnicos
- Medios humanos
- Medios administrativos

Las acciones que se prevean implantar para fortalecer la seguridad de los sistemas se relacionarán en la tabla siguiente:

TABLA 5

Sistema (denominación)

ACCIONES A TOMAR	PLAZO DE EJECUCION	RECURSOS NECESARIOS	RESPONSABLE
(preventivas, detectivas, recuperativas)	(Si hace falta, se precisan las etapas)	(Técnicos, humanos. Financieros, etc.)	

Las acciones preventivas y recuperativas que se implementen se incluirán en el Plan de Contingencias, donde deben ser definidos de forma precisa, para cada una de las contingencias previstas, los siguientes aspectos:

¿Qué hacer durante una contingencia?

¿Quién lo hace?

¿Cómo y con qué recursos?

6.3. Tercera Etapa. Evaluación del sistema diseñado.

La evaluación del sistema de seguridad diseñado consiste en la determinación de la capacidad del mismo para impedir la materialización de las amenazas de la forma más efectiva y racional. En esencia su realización estriba en la comparación de los resultados obtenidos en el análisis de riesgos con las políticas y acciones que han sido implementadas, validando como las mismas logran minimizar los riesgos estimados de forma rentable.

En general el costo de proteger los bienes informáticos debe ser menor que el costo de la recuperación y es por ello que los riesgos deben ser clasificados por su nivel de importancia y por la severidad de la pérdida que puedan ocasionar.

Durante el proceso de evaluación es necesario establecer si se ha logrado una correspondencia adecuada entre las políticas de seguridad definidas y las acciones que garantizan su implementación. Como regla, cada una de las políticas definidas debe estar respaldada por las acciones que le correspondan en las diferentes áreas y del mismo modo, no deben existir acciones que no estén fundamentados en alguna política.

El proceso de evaluación se realiza de manera continua, a partir de que las condiciones que determinan el sistema de seguridad varían constantemente por causa de múltiples factores, como son la introducción de nuevas tecnologías y servicios o el cambio de sus características de explotación, la entrada o salida de personal, los cambios en la ubicación del equipamiento, el descubrimiento de vulnerabilidades no previstas, etc.

Un caso a tener siempre presente es cuando se produce un incidente de seguridad (contingencia), a partir del cual es imprescindible tomar un conjunto de acciones dirigidas a determinar las causas que lo propiciaron y los cambios que son necesarios realizar en el sistema de seguridad para que el mismo no se vuelva a repetir.

Cada vez que se produzca un cambio en las condiciones que determinaron el sistema de seguridad diseñado se debe realizar un nuevo análisis de riesgos a fin de precisar como éste ha sido afectado y realizar los ajustes correspondientes.

Las acciones anteriores proporcionan una realimentación del sistema de seguridad que posibilita su reevaluación y perfeccionamiento constante.

7. Organización del trabajo

- ✓ Cada Organismo creará una comisión central presidida por un dirigente del primer nivel, de la cual formen parte el órgano de Seguridad y Protección, el órgano rector de la Informática y representantes de aquellas áreas con mayor incidencia en los procesos de gestión de la información.

- ✓ Se crearán además tantas comisiones como se requiera para la ejecución del trabajo en áreas funcionales o ramas.

- ✓ Al finalizar cada una de las etapas de trabajo se realizará una revisión de la misma por la comisión central de cada Organismo.

7.1. Etapas de realización

El trabajo se organizará en cada Organismo en tres etapas, en los plazos previstos en el cronograma que se anexa. Las etapas serán las siguientes:

1) Determinación de las necesidades de protección.

    - Caracterización del entorno informático.
    - Identificación de amenazas y estimación de riesgos.
    - Evaluación actual de la seguridad.

2) Definición e implementación de las acciones que garanticen minimizar los riesgos.

    - Medios técnicos, recursos (financieros, humanos, etc), acciones.

3) Evaluación de las soluciones diseñadas.

Anexo 1

ADMINISTRACION DE CONTINGENCIAS

Los aspectos principales a tener en cuenta al establecer la política a seguir para el tratamiento (administración) de contingencias son:

- Determinación de los objetivos de la administración de contingencias.
- Evaluación de contingencias (cuan seria es la contingencia).
- Reporte de contingencias (quien debe ser notificado sobre la misma).
- Respuesta a las contingencias.
- Documentación de contingencias.
- Procedimientos post- contingencias.

OBJETIVOS DE LA ADMINISTRACION DE INCIDENTES

- Asegurar la integridad de los sistemas críticos.
- Mantenimiento y restauración de los datos.
- Esclarecer como fue que sucedió.
- Evitar el escalamiento e incidentes adicionales.
- Estimar el impacto de la contingencia.
- Recuperarse de la contingencia.
- Encontrar quien la ocasionó.
- Castigar al atacante.
- Encontrar la forma de evitar la explotación futura de las mismas vulnerabilidades.
- Actualizar las políticas y los procedimientos que sean necesarios.
- Evitar una publicidad negativa para la entidad.

PRIORIDADES PARA LA ADMINISTRACION DE CONTINGENCIAS

1) Proteger la vida humana y la seguridad de las personas (la vida humana siempre tiene precedencia sobre cualquier otra consideración).

2) Proteger la información clasificada o limitada (reguladas por el Organismo o estatalmente).

3) Proteger otras informaciones (de administración, científicas, propietarias, etc.).

4) Prevenir daños al sistema (pérdida de ficheros, daños a discos, etc.).

5) Minimizar la interrupción de los recursos de cómputo.

Parte de la administración de contingencias es estar preparado para responder antes de que el incidente ocurra. Esto determina el establecimiento de niveles aceptables de protección de forma tal que si el incidente es severo, los daños que puedan ocurrir sean limitados. La protección incluye la determinación de los principios o lineamientos adecuados (política) para manejar incidentes y la elaboración de un plan de contingencia para la entidad. De esta forma se eliminan muchas de las ambigüedades que ocurren durante un incidente y se logrará un conjunto de respuestas más apropiadas.

También es necesario preparar un método para el reporte de los incidentes, de forma tal que se pueda conocer y tener determinado a quien llamar y como contactarlo.

La entidad debe establecer los procedimientos de salva de la información para cada máquina y sistema, lo que minimiza muchas de las amenazas, aun incluso en incidentes severos.

Es imprescindible establecer sistemas seguros, lo que implica la eliminación de vulnerabilidades, el establecimiento de una efectiva política de control de acceso y otros procedimientos.

Debe ser considerado la utilización de mecanismos de detección (auditoría y alarmas, monitoreo, etc.) que permitan conocer a tiempo la ocurrencia de un incidente de seguridad y el establecimiento de los procedimientos de gestión adecuada de esos mecanismos.

Hay que establecer un programa de entrenamiento como parte de la protección que incluya la simulación de incidentes y su tratamiento.

EVALUACION DE CONTINGENCIAS

La evaluación de contingencias consiste en la determinación exacta del problema. Muchos de los indicios frecuentemente asociados con infección por virus, ataques al sistema, etc., son simplemente anomalías tales como fallos del hardware. Como medio de ayuda para determinar si lo que en realidad está pasando es un incidente es posible obtener y emplear algún software de detección que pueda estar disponible, por ejemplo un programa antivirus. La información de auditoría es también extremadamente útil, en especial para determinar si hay un ataque a la red.

El empleo de estos recursos es muy importante para obtener una “instantánea” del sistema tan pronto se sospeche que algo anda mal. Muchos incidentes provocan la ocurrencia de una cadena dinámica de eventos y una “instantánea” inicial del sistema es mejor en la identificación del problema y las fuentes de ataque (origen) que otras muchas acciones que pudieran ser tomadas en esta etapa.

Durante la evaluación de la contingencia hay que hacer una caracterización de la misma, determinando en que consistió, donde y cuando ocurrió, en que forma se produjo, como fue detectada y cualquier otro aspecto que pueda resultar de interés.

También en esta etapa es importante comenzar a registrar los eventos del sistema, conversaciones telefónicas y otros aspectos que pueden permitir una más rápida y sistemática identificación del problema y es la base para las etapas subsiguientes del tratamiento de contingencias.

INDICIOS MAS FRECUENTES

- Caída del sistema.
- Nuevas cuentas (inexplicables) de usuarios.
- Gran actividad de cuentas que durante largo tiempo han estado inactivas.
- Nuevos ficheros (usualmente con nombres nuevos o extraños).
- Discrepancias de contabilidad.
- Cambios de longitud de ficheros o datos.
- Intentos de escritura en el sistema.
- Modificación o borrado de datos.
- Denegación de servicios.
- Empeoramiento inexplicable del rendimiento del sistema.
- Aparición de anomalías.
- Pruebas sospechosas (numerosos intentos de logins infructuosos)

Ninguno de estos indicios es una prueba absoluta de que está ocurriendo un incidente ni son todos estos indicios normalmente observados cuando se produce un incidente, pero si se observa alguno de ellos hay que sospechar que un incidente está teniendo lugar y actuar en correspondencia.

Parte de la identificación del incidente es la evaluación del alcance y el impacto del problema. Es importante la determinación correcta de los límites del incidente en interés de darle un tratamiento efectivo. Adicionalmente el impacto de un incidente determinará las prioridades en la asignación de recursos para tratarlo. Sin una clara determinación del alcance y del impacto es difícil determinar una respuesta adecuada.

CRITERIOS PARA DETERMINAR EL ALCANCE Y EL IMPACTO

- ¿Es un incidente multisitio?
- ¿Hay muchas PC´s afectadas por el incidente?
- ¿Hay involucrada información clasificada o limitada?

- ¿Cuál es el punto de entrada del incidente? (red, línea telefónica, terminal local, etc.)
- ¿El incidente ha transcendido la entidad?
- ¿Cuál es el daño potencial del incidente?
- ¿Cuál es el tiempo estimado para neutralizar el incidente?
- ¿Qué recursos serán requeridos para manejar el incidente?

RESPUESTA A LAS CONTINGENCIAS

En dependencia del momento en que se apliquen y su vigencia las acciones de respuesta a una contingencia pueden ser: **Inmediatas** (Ej: Abortar inmediatamente las operaciones mediante la desconexión); **Temporales** (Ej: Invalidación temporal de alguna entidad o cuenta de usuario); **A largo plazo** (Ej: Introducir una entidad en una "lista negra" o el cambio de una clave).

En base al contenido de las acciones a realizar, durante la respuesta a una contingencia pueden ser definidas las siguientes etapas:

- Contención
- Erradicación
- Recuperación
- Seguimiento

CONTENCION

Consiste en limitar la extensión de un ataque. Una parte esencial de esta etapa es la toma de decisiones, algunas de las cuales podrían ser: apagar el sistema; desconectarse de la red; suprimir funciones, establecer trampas, etc. Algunas de estas decisiones son triviales, por ejemplo desconectar el sistema si hay información clasificada o limitada o si la información propietaria está en riesgo. En otros casos hay que valorar asumir el riesgo de algunos daños en interés de identificar al intruso.

Para esta etapa deben tenerse previstas las estrategias y acciones adecuadas y los procedimientos a seguir, así como la información que debe ser brindada a quien corresponda.

Es importante en esta etapa tomar medidas para garantizar la preservación de las condiciones existentes en el momento en que se produjo la contingencia, lo cual es de suma importancia para las acciones posteriores.

ERRADICACION

Una vez que la contingencia ha sido contenida es necesario erradicar los problemas que ésta ha causado. Para ello puede que haya disponible algún software apropiado, por ejemplo un software antivirus, si ese es el caso. Si como

resultado del incidente algún fichero problemático ha sido creado, este es el momento de borrarlo.

RECUPERACION

El objetivo de la etapa de recuperación es regresar el sistema a su estado normal de funcionamiento y eliminar las causas que lo propiciaron.

En el caso de un ataque a redes es importante instalar los “parches” adecuados para eliminar cualquier vulnerabilidad del sistema operativo que haya sido explotada.

SEGUIMIENTO

Es una de las etapas más importante en la respuesta a una contingencia y también muy frecuentemente omitida. Su principal importancia reside en que las experiencias que se obtienen ayudan a mejorar la forma de actuar ante futuras situaciones similares y al mismo tiempo proporcionan información que justifica el esfuerzo a realizar en materia de seguridad en una entidad, lo cual puede resultar esencial en procedimientos legales, si éstos tuvieran lugar.

El elemento más importante en la etapa de seguimiento es la realización de un análisis “post-mortem” que consiste en precisar:

- ¿Qué paso exactamente y en que momento?
- ¿Cuan involucrado estuvo el personal (staff) en el desarrollo del incidente?
- ¿Qué clase de información se necesitó rápidamente y como se pudo obtener oportunamente?
- ¿Qué se hará diferente la próxima vez?

Un reporte de esta etapa es valioso porque proporciona una referencia de gran utilidad en caso de otra contingencia similar. La creación de una cronología de los eventos es también importante por razones legales. Esto es también útil con vistas a obtener un estimado económico de los daños causados por la contingencia en término de cualquier pérdida de software y ficheros, hardware y costos de la fuerza de trabajo empleada para restaurar ficheros alterados, reconfigurar sistemas afectados, etc.

DOCUMENTACION DE LAS CONTINGENCIAS

Durante el desarrollo de una contingencia deben registrarse todos los detalles relativos a la misma. Esto garantiza una valiosa información para todos los que de una forma u otra tengan que relacionarse con los eventos que se van produciendo, evitando pérdidas de tiempo. Un registro detallado de estos eventos proporciona evidencias para ser usadas en un posible proceso legal y además facilita una estimación más exacta de los daños y garantiza la base para el análisis posterior de las experiencias acumuladas durante la contingencia.

Como mínimo deben ser registrados:

- Todos los eventos del sistema (trazas de auditoría).
- Todas las acciones tomadas (y la hora en que fueron tomadas)
- Todas las conversaciones telefónicas, incluyendo las personas con quien se habló, la fecha, la hora y el contenido.

Debe ser habilitado un libro de registro que permita tener una fuente de información cronológica y centralizada cada vez que se necesite.

REPORTE DE LAS CONTINGENCIAS

Al confirmarse que una contingencia está ocurriendo debe informarse al personal apropiado, para lo cual es importante tener determinado de antemano a quien y como debe ser brindada esta información a fin de mantener el incidente bajo control desde el punto de vista técnico y emocional. Para ello debe tenerse en cuenta lo siguiente:

- La información que se brinde al personal local o externo debe ser **explícita**. Esto implica que cualquier información sobre la contingencia, independientemente de la vía que se utilice (teléfono, fax, correo electrónico, etc.) debe ser **clara, concisa, calificada y completa**. Cuando se informa a otros que prestarán ayuda en el tratamiento de la contingencia una "cortina de humo" solo dividirá los esfuerzos y creará confusión.

- La información debe ser **veraz y objetiva**. El intento de ocultar aspectos de la contingencia proporcionando información falsa o incompleta puede no solo impedir una solución acertada a la misma, sino incluso empeorar la situación.

- La selección del lenguaje utilizado para informar sobre la contingencia tiene también gran importancia. El empleo de términos inadecuados, de forma oral o escrita, puede crear alarmas infundadas o falsas expectativas sobre el impacto del incidente. Una especial atención debe prestarse a la selección del lenguaje utilizado para informar al personal no especialista a fin de no crear confusión.

- ¿Quién debe ser informado durante y después de la contingencia? En este aspecto hay que considerar las siguientes categorías de personas que deben ser informadas:

    - Personal técnico.
    - La administración de la entidad.
    - Equipos de respuesta.
    - Autoridades estatales.
    - Proveedores.

Una lista de las personas de cada una de estas categorías que deben ser informadas puede ser muy útil durante una contingencia, cuando se están desarrollando muchos eventos de urgencia.

Adicionalmente a las personas involucradas con el tratamiento de la contingencia, puede haber otros sitios afectados (o simplemente en riesgo de ser afectados) que serían beneficiados si se les informa sobre el incidente. Con frecuencia resulta apropiado, una vez que la contingencia ha concluido, informar del mismo a la comunidad de usuarios.

PROCEDIMIENTOS POST-INCIDENTES

Una vez que la contingencia ha sido resuelta deben ejecutarse las siguientes acciones:

1) Un inventario de los activos del sistema, es decir hacer un examen minucioso para determinar como fue afectado el sistema por la contingencia.

2) Las experiencias obtenidas como resultado de la contingencia deben ser registradas y conservadas y por supuesto tienen que ser tomadas en cuenta en la revisión del Plan de Seguridad a fin de prevenir que no vuelva a ocurrir.

3) Deben ser determinadas las causas y condiciones que propiciaron la contingencia o que limitaron la capacidad de obstaculizarla, precisando al mismo tiempo la existencia de otras posibles vulnerabilidades.

4) Hay que desarrollar un nuevo análisis de riesgos a la luz de la contingencia y a partir de sus resultados y de las experiencia obtenidas durante la misma actualizar las políticas y procedimientos de seguridad..

5) Hay que investigar los antecedentes de la contingencia, precisando si con anterioridad habían ocurrido otras de la misma naturaleza, tanto en el lugar como en otras entidades y la forma y circunstancias en que se produjeron.

6) Debe determinarse si es necesaria la ejecución de medidas adicionales como pudieran ser la realización de una auditoría específica a una parte o a todo el sistema de seguridad que resultó violado u otras medidas operativas complementarias.

7) Debe realizarse la investigación y procesamiento (si se considera apropiado) de los individuos que causaron la contingencia.

Las acciones anteriores proporcionan una realimentación a la Política de Seguridad que posibilita su reevaluación y perfeccionamiento. Para su realización debe ser creada una comisión de investigación designada por la dirección de la entidad e integrada por un representante del Organo de Protección de la entidad, el Responsable de Seguridad Informática y al menos dos personas más que cuenten con los conocimientos técnicos e informativos del área donde se ha producido el incidente, siempre que no estén implicados en el mismo.