Evaluación de riesgos en las tecnologías en Cuba

Rodney A. López Rodríguez

rlopez@vertice.cu

Fecha Publicación: 15/01/2009

Resumen

La evaluación de riesgos en las tecnologías de la información así como el enfoque dado a su uso en Cuba está plagado de subjetividad y carece de un enfoque estadístico y de gestión adecuados. Es por eso que en nuestro trabajo basándonos en el estudio del contexto de operaciones, de principios establecidos para la gestión TI y un enfoque estadístico nos planteamos la creación de un marco auditable de subjetividad reducida para la evaluación de los riesgos.

Palabras Clave

Convergencia: Enfoque único de la seguridad dentro de la organización con el objetivo de crear mecanismos más efectivos e involucrar a todas las partes en un ambiente cooperativo para enfrentar amenazas comunes.

Procesos: Unidad lógica/organizacional determinada por elementos de entrada que a través de un conjunto de actividades se transforman en elementos de un conjunto de salida. Para desambiguar posibles caracterizaciones para un mismo proceso utilizamos el concepto de proceso atómico, elemental o básico que es aquel conjunto minimal de actividades que devuelvan un resultado de valor a al menos un actor.

Alineación: (de los objetivos) Correspondencia entre los objetivos generales de la organización y los de cada área de la misma.

Factor de Riesgo: Característica propia del sistema que lo hace más vulnerable a una amenaza específica y que a su vez influye en alguno de sus atributos básicos.

Amenaza: Evento del sistema que puede influir de manera negativa en el esquema de gestión.

Métricas: Estadígrafo, medida de la eficacia de los esfuerzos en seguridad de una organización a lo largo del tiempo.

1. INTRODUCCIÓN

La evaluación de riesgos cobra cada vez mayor protagonismo como herramienta a la hora de desarrollar un sistema de gestión de seguridad sea en las tecnologías de la información o en cualquier otra rama científico, económica o social.

Según Dan Geer la subjetividad es inherente al análisis de la seguridad, sin embargo es nuestro deber desarrollar metodologías lo más objetivas posibles para obtener los resultados más precisos que nos permitan desarrollar una estrategia de securización adecuada.

Hoy el mundo de la seguridad muestra conceptos nunca pensados tiempos atrás y cada vez más las tendencias en las amenazas nos obligan a enfocarnos en las personas y en nuestro propio sistema pues si bien la seguridad se basaba en el estudio de elementos externos que nos amenazaban hoy se ha demostrado que son las características internas de nuestras redes las que nos hacen más vulnerables o no a los incidentes de seguridad.

En Cuba nos queda un trecho largo por avanzar en seguridad TI y es quizás en la evaluación de los riesgos uno de los caminos más largos que nos quedan. En primer lugar hay que garantizar que las metodologías y regulaciones lleguen a todos los involucrados con esta actividad y en segundo, tercero y más, nos queda mirar más hacia la organización, dándole un adecuado enfoque de análisis de los procesos, la reducción de la subjetividad y en general brindar a las organizaciones un resultado de valor que constituyan valga la redundancia un valor agregado a nuestros productos o servicios.

Es por eso que nos planteamos en nuestro trabajo la creación de un marco de evaluación auditable que nos permita reducir la subjetividad mediante un análisis holístico de todos los elementos tratando de no complejizar el proceso para lograr el máximo de operatividad. Todo esto mediante el uso de herramientas y principios establecidos y de reconocida eficacia en todo el mundo.

Para nosotros la colaboración y la comunicación constituyen una parte fundamental del análisis pues a través de la experiencia diaria hemos observado que la capacidad de establecer un sistema efectivo es directamente proporcional a la habilidad de cooperación de las partes involucradas.

Un aspecto que nos pareció revelador en el trabajo de A. Corletti y que incorporamos a nuestra metodología son los criterios de envejecimiento de la tecnologías lo cual nos permite el aumento de la precisión en los cálculos de la evaluación.

Para un modelado más preciso del contexto de operaciones nos auxiliamos del UML y de técnicas y herramientas de ingeniería de software que nos permite capturar las reglas del negocio e identificar y caracterizar los procesos de una manera detallada

Si bien esta metodología no ha sido utilizada para realizar una evaluación independiente los principios establecidos en ella se usaron como metodología de apoyo a la evaluación de riesgo realizada en VERTICE que se presento en el XVI Forum de base bajo la denominación MAPER 0.6.

2. METODOLOGÍA

2.1 Elementos generales

La visión de la seguridad implícita en esta exposición es la de un conjunto de estados definidos por las configuraciones a través de los cuales el sistema transita en respuesta a eventos.

La evaluación de riesgos y del estado de seguridad ha dejado de ser una ciencia meramente técnica para convertirse en todo un arte que involucra la pericia técnica, conocimiento organizacional y la habilidad de comunicación.

La convergencia de la seguridad en una organización se hace cada vez más necesaria pues permite no solo un ahorro considerable de tiempo, esfuerzos y recursos sino que permite enfrentar las amenazas de manera más efectiva al involucrar acciones coordinadas de las partes involucradas. Actualmente en nuestras empresas hablamos de control interno, plan de prevención, seguridad y protección y seguridad informática pero no siempre se ven como un todo interrelacionado que nos permite garantizar la continuidad de las operaciones.

En nuestro sistema se interrelacionan elementos con características disímiles y es nuestra obligación realizar una evaluación con un enfoque sistémico, pero vamos a encontrar dificultades en las diferencias de los lenguajes, métodos y objetivos entre las diferentes áreas y aun especialistas.

Es por eso que luego del análisis de las características de los sistemas de seguridad y sus partes elementales así como la organización del control establecida en el país nos propusimos la subdivisión del sistema en 3 capas : física, lógico técnica y organizacional las cuales cuentan con las características siguientes:

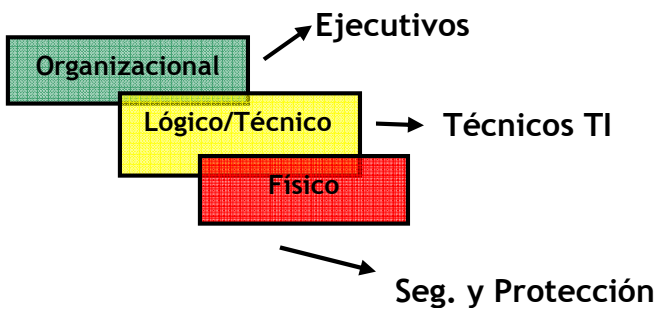

Fig.1

1. La subdivisión del sistema nos permite garantizar a la vez que simplifica el proceso de convergencia de los intereses de seguridad.

- Física: Pertenecen todo lo material y lo relativo a la protección del mismo. Es importante a la hora de realizar el análisis de esta capa realizarlo de conjunto con el jefe de seguridad y protección.
- Lógico/Técnico: Enmarca los paquetes de aplicaciones, configuraciones, almacenamiento lógico de información y semejantes. En esta capa es vital el contacto con el grupo de gestión TI.
- Organizacional: Pertenecen los procesos, servicios, la información como tal, los roles, objetivos y semejantes. Es imprescindible el contacto con los ejecutivos, dígase auditores, directores o jefes.

Con esta subdivisión buscamos optimizar el tiempo de contacto y mantener en foco en el tema de cada especialista aunque no descartamos los contactos en un marco más amplio que permitiera una coordinación más profunda del análisis. Luego nos corresponde a nosotros juntar las piezas de este rompecabezas de una manera tal que obtengamos los resultados óptimos en nuestra evaluación.

Cuando hablamos de evaluación de seguridad realmente es como si hablásemos de un 3x1, la **seguridad mostrada**, relacionada con la frecuencia de los eventos y la exposición del sistema, la **seguridad detectada** que se relaciona con la habilidad para capturar el estado de seguridad y la eficacia de los controles, ambas como percepción de la **seguridad real**, diferencias ostensibles entre "las 3 seguridades" conllevan a falsas expectativas o desgaste.

2.2 Estudio del Entorno del Negocio

2.2.1 Caracterización del entorno de operaciones

Durante la fase de diseño el sistema está sujeto a la influencia del ambiente psico-social y económico el que condiciona la concepción de la misión de la organización así como más tarde la percepción de esta.

Es importante que se conozca tanto la misión, como la visión y los requisitos formales e informales de manera que se establezca una correlación entre los objetivos generales y nuestros objetivos y así evitar el riesgo mayor :Que no se haga lo que se debería hacer.

Por otra parte esto nos permitiría definir causas objetivas y una mejor caracterización del entorno de operaciones lo cual conlleva a un proceso de identificación de eventos y a la definición de criterios de riesgos más precisos.

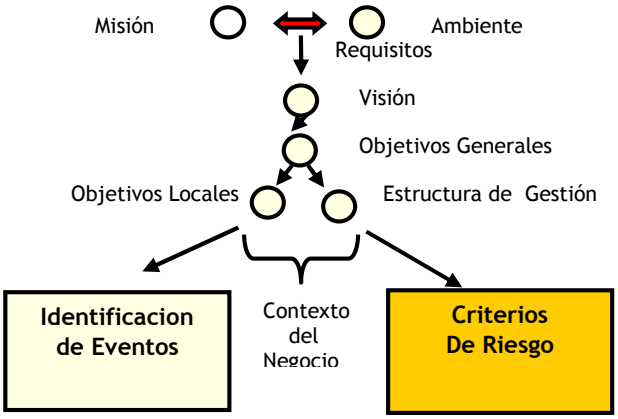

Fig.2. El diseño de la organización es una parte fundamental de la Gestión de riesgos

Todos estamos acostumbrados a observar el uso de la matriz DAFO para definir nuestro entorno de operaciones y si la completamos a partir de un estudio que nos interrelacione los objetivos a distintos niveles, la estructura de gestión y los eventos ya sean en el marco más general de la sociedad, en el más cerrado del sector productivo o en el particular de la organización.

El estudio del contexto del negocio y dentro de este más específicamente los objetivos y la estructura de gestión nos debe permitir elaborar nuestros criterios de riesgos evitando el mal tan común de la "asimilación indiscriminada" por parte de nuestras organizaciones.

Es importante para obtener una información más objetiva determinar el nivel de alineación de los objetivos de la seguridad con los objetivos de cada área es por eso que usamos el siguiente diagrama donde establecemos la correspondencia entre los objetivos generales, los de cada área y los del área de seguridad TI.

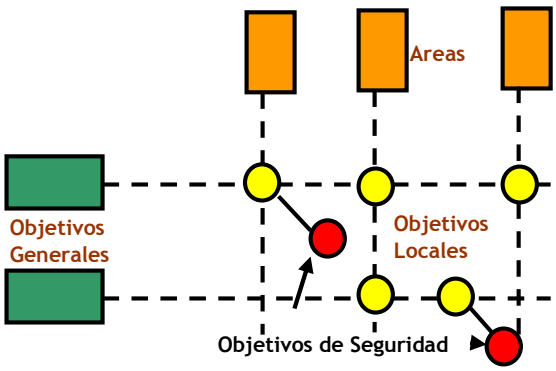

Fig.3. Análisis de la alineación de los objetivos TI con los objetivos del negocio.

Esto nos permitirá detectar desviaciones hacia aspectos no priorizados por la organización y una mejor organización de la gestión de riesgos.

Así mismo el estudio de esta etapa nos permitirá de conjunto con el estudio más adelante del contexto del negocio realizar una identificación de nuestros eventos más significativos de manera que podamos determinar nuestras amenazas, oportunidades, fortalezas y debilidades de una manera tan objetiva como queramos.

En la fase de identificación de los procesos se procede a realizar los diagramas de casos de uso esto nos permitirá aislar los procesos más simples y obtener información básica de las interrelaciones del sistema.

Durante la fase de análisis de los procesos el uso de los diagramas de actividad nos permite obtener una información tan detallada como queramos del funcionamiento de los procesos permitiéndonos detectar un diseño defectuoso.

El análisis de la interrelación de los procesos se debe realizar teniendo en cuenta la información y los sistemas encargados de su elaboración, almacenamiento, transmisión y modificación

La jerarquización de los procesos la realizamos teniendo en cuenta dos aspectos: La madurez operativa y su clasificación. La priorización de los procesos la realizamos teniendo en cuenta dos aspectos: La madurez operativa y su clasificación, mediante la fórmula:

$P_i = M.C$ (1)

Donde P_i corresponde a la prioridad del proceso i

- M: Madurez operativa esta toma los valores:
  - Integrado : 1.0
  - Semi-aislado : 0.6
  - Aislado : 0.3
- C: Clasificación:
  - Básico :1.0
  - Básico alternativo :0.7
  - Control :0.25
  - Soporte :0.2

Los valores otorgados persiguen ponderar los valores extremos de manera que ningún proceso básico obtenga una prioridad inferior que un proceso de soporte.

Este cálculo nos permitirá el uso de un coeficiente auxiliar en el momento de calcular la importancia de los bienes sujetos a la evaluación, además de ser un indicador de la criticidad de la estructura.

Durante esta etapa el conocimiento de alguna herramienta de modelado es esencial o algún lenguaje de modelado ya que nos permite

capturar con gran eficiencia la información, en nuestro y por ser probadamente exitoso su uso en el entorno empresarial internacionalmente escogimos UML.

La evaluación de la gestión TI se realiza para determinar cuan preparada se encuentra la organización para enfrentar los cambios que se generan en el sistema y la capacidad de respuesta de esta:

- **Valor:** Enlace entre las métricas TI y las del negocio, impacto de mejora de las TI en el negocio, infraestructura de tiempo real y planificación del negocio.
- **Servicio:** Define servicios, clases, precios, comprensión de los costos, establecimiento de métricas de calidad, garantías de niveles de servicio, monitoreo/reporte de lo servicios y planificación de la capacidad.
- **Proactivo:** Monitoreo de ejecución, análisis de tendencias, establecimiento de umbrales, predicción de problemas, automatización y gestión del cambio y demás.
- **Reactivo:** Mejor esfuerzo, "apagafuegos", inventario, gestión de problemas básica, gestión de eventos y alertas y monitoreo de la disponibilidad.
- **Caótico:** Ad hoc, sin documentación, impredecible, múltiples helpdesk, operaciones TI mínimas y notificación del usuario.

Durante esta etapa debemos elaborar el mapa de la red y los servicios TI así como realizar el análisis de su funcionamiento. Esto nos permitirá determinar los posibles puntos de ruptura, límites y puntos de acceso.

2.2.2 Orientación a procesos

"La aplicación de un sistema de procesos dentro de la organización junto con la identificación e interacción de estos procesos, y su gestión es conocida por "orientación a procesos" [1].

Acorde a esta definición brindada por la norma ISO queda bien claro lo que es una orientación a procesos pero podríamos preguntarnos ¿Qué es un proceso? ¿Por qué adoptar un enfoque de gestión orientado a procesos?

Según la misma norma ISO un proceso no es más que: "Cualquier actividad usando recursos y gestionado con el propósito de transformar una entrada en una salida". He ahí tres palabras fundamentales que nos dan el por qué: Actividad, recursos y gestionado (gestión) y es que un proceso es una unidad dentro de la cual estructuramos de una manera lógica el funcionamiento de la organización, permitiendo organizar de una mejor manera los recursos materiales y humanos, facilitando el análisis de la eficacia y eficiencia de las tareas acometidas: "Si la estrategia nos dice que es lo que hay que hacer para alcanzar los objetivos fijados, los procesos nos ayudan a hacerlo con eficacia" [2].

Sin embargo la antedicha definición de procesos carece de rigurosidad y esto puede hacernos fracasar al depender del índice de

experticidad de la persona responsabilizada con la identificación y caracterización de los procesos dado el carácter relativo con respecto al observador que poseen los procesos. Esto puede conllevar a que se pierdan detalles significativos, dígase flujos de información, recursos o actividades y relaciones entre puestos de trabajo. Es por eso que utilizamos el concepto de proceso simple o atómico definido como: El conjunto minimal de actividades que refleja un algoritmo de trabajo usando recursos, gestionándolos, que tiene como objetivo transformar una entrada en una salida que refleja desde el punto de vista de al menos un actor un resultado de valor.

La orientación a procesos propugnada por los estándares ISO enfatizan en la importancia de:

1. Conocer los requerimientos de la organización y la necesidad de establecer políticas y objetivos.

2. Implementar y operar controles para administrar la organización en el contexto general en que se ubica.

3. Monitorear y revisar la efectividad de la organización

4. Mejora contínua basada en la medición de los objetivos.

Según [2] la tradicional orientación de las empresas hacia la jerarquía ha conducido a una fuerte especialización que se aleja cada vez más del cliente y genera altos costos por necesidades de coordinación. Sin embargo la orientación a procesos pone el foco de atención en la prioridad número uno: la satisfacción del cliente y a este como principal objetivo de nuestra gestión.

Si bien el despliegue de políticas sirve para comunicar verticalmente los objetivos principales de la organización los procesos difunden las necesidades de los clientes de manera horizontal. “La conjunción de ambos despliegues proporciona la cohesión que se necesita para orientar los esfuerzos de mejora” [2].

El proceso simple es el núcleo fundamental de funcionamiento de la empresa es por eso que escogimos como dominio de riesgo a los procesos. El estudio detallado de estas unidades de operación permite definir claramente las características del negocio.

Esto por otra parte nos permite ofrecer un resultado para cada servicio al ser estos, expresión del resultado de un proceso.

2.2.3 *Papel de la información*

En la gestión empresarial actual la información tiene la capacidad de entorpecer o facilitar de manera determinante el funcionamiento de la organización de ahí que la Gestión de TI alcance un peso imposible de obviar en las mismas.

La información es el mínimo común denominador a todos los procesos y sus componentes dentro de la organización sea cual fuere su tipo y refleja las características generales del funcionamiento de la

empresa. Analizando su ciclo de vida se puede determinar el nivel de actividad de una organización.

El ciclo de vida de la información se puede dividir en dos etapas básicas la **activa** y la **pasiva**. En la etapa activa la información forma parte de los procesos productivos y jugando un papel fundamental en el cumplimiento de los objetivos empresariales; por otra parte en su etapa pasiva la información forma parte de mecanismos de consulta o referencia o es evidencia legal o formal del funcionamiento de la producción; más que una simple categorización esto refleja la capacidad de la información de afectar directa o indirectamente el flujo de trabajo.

La importancia de determinar el tiempo de vida de la información está relacionada con la capacidad de enmarcar los ciclos de controles así como una más efectiva distribución de estos y en general de los recursos.

Uno de los mayores riegos que corre el uso eficiente de la información y los recursos asignados a su preservación es la descontextualización, que se manifiesta generalmente en la diferencia entre el ciclo de vida práctico y el establecido para las salvas, la pérdida de significado y el uso ineficiente de los recursos asignados a la conservación de esta.

A partir del estudio del flujo, ciclo de vida y demás características de la información se identificaran un gran número de factores de riesgo del sistema.

2.3 Evaluación de Riesgos

2.3.1 Factores de Riesgo

Los factores de riesgo como aparece escrito en el acápite de palabras claves son aquellas características propias del sistema -nunca eventos- que influyen en los atributos básicos de una amenaza y que por lo tanto su conocimiento nos permitirá ser más capaces de establecer mecanismos de mitigaron de las amenazas.

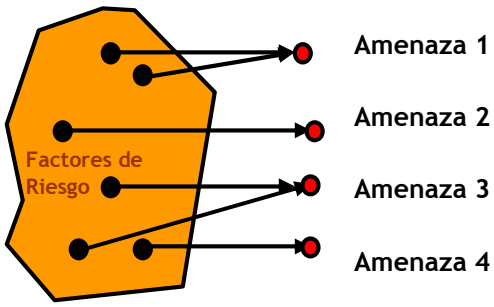

Fig.4

Los eventos no pueden constituir factores de riesgos pues en si ellos tipifican transiciones entre estados y desde el punto del análisis pudieran generar ambigüedad.

Los factores según los atributos de las amenazas que influyan se pueden clasificar en los siguientes grupos no mutuamente excluyentes:

Intensidad: Son aquellos que influyen sobre el impacto de una amenaza en el sistema.

Duración: Aquellos que determinan el intervalo de tiempo de eficacia de una amenaza una vez materializada.

Frecuencia: Aquellos que determinar cuántas veces en un periodo determinado de tiempo se materializara una amenaza.

Timing: Aquellos que influyen en el momento en que se materializara la amenaza.

Cuando se analizan los factores de riesgo que influyen sobre una amenaza puede ser aconsejable la subdivisión en conjuntos de factores necesarios y/o suficientes, facilitando la tarea de mitigar los riesgos y a la hora de determinar el origen de un incidente nos puede ayudar sobremanera realizar este análisis preliminar.

Existen categorías especial de factores de riesgo unos son aquellos que influyen en la interrelación entre procesos pues constituyen factores de propagación de las amenazas y otros son los factores que influyen en los riesgos inherentes a los controles.

Para que se materialice una amenaza deben existir tres elementos básicos: la **capacidad**, la **necesidad** y la **oportunidad**. Comprendiendo esto podemos realizar una agrupación de los factores de riesgos de manera que podamos establecer una mejor estrategia de mitigación a partir de identificar el blanco de nuestras acciones y poder establecer una correspondencia entre el esfuerzo y el gasto financiero a realizar.

2.3.2 Amenazas

Las amenazas según sus causales pueden clasificarse en accidentales o intencionales y estas últimas a su vez en internas, externas o internas-externas, más que una simple clasificación esto nos permite determinar elementos de los criterios de medidas que debemos elaborar.

Una forma de facilitar la clasificación de las amenazas según esta escala es la de asociar a la amenaza su agente, en reciprocidad obtenemos un dato esencial para utilizar en el momento de elaborar nuestras contramedidas.

He sido testigo de una tendencia a encasillar las amenazas y darle un enfoque genérico, esta de mas decir que mientras más generales sean las definiciones de las amenazas más generales van a ser en correspondencias las estrategias de mitigación y por tanto menos efectivas.

En la evaluación de riesgos la amenaza constituye la variable estadística a estudiar y es por eso que al construir la escala donde cada amenaza equivale a una clase es importante que se cumplan los principios de exclusión mutua y exhaustividad, caso contrario los resultados obtenidos estarían lejos de estar correctos. Una herramienta muy útil a la hora de realizar este proceso son los grafos de ataque y podemos utilizar cada camino del grafo hasta un estado final como una clase para nuestra escala.

No debemos detenernos en simplemente identificar las amenazas sino que debemos seguir nuestro análisis y determinar las causas primarias de las mismas determinar cuáles constituyen factores de riesgos y cuales son modificados a partir de otras amenazas.

2.3.3 Calculo del riesgo

El cálculo del riesgo no es más que el cálculo del valor esperado de una variable aleatoria. Lejos de encasillarnos en un simple calculo debemos explotar todas las medidas que nos brinda la estadística a la hora de analizar una variable aleatoria dígase media, moda, mediana, varianza en fin cada una adquiere un significado particular en nuestro análisis permitiendo enriquecerlo en la misma medida en que seamos capaces de asimilarlas e interpretarlas.

2.4 Comunicación de los resultados

Toda vez realizado el análisis viene una etapa crítica que puede malograr todos nuestros esfuerzos gastados durante la evaluación: La presentación de los resultados.

Uno de los principales problemas es encontrar un lenguaje común con el personal no especialista de las TI, que no sea técnicamente críptico pero que a la vez posea la rigurosidad técnica que amerita.

Las representaciones graficas de la información constituyen una herramienta muy útil al presentarla en un entorno simple y atractivo.

A continuación listamos algunos de estos y la información que puede brindarse a través de ellos:

Dispersión: nos permiten realizar un mapa de riesgos donde se muestren de manera visual y atractiva la criticidad del sistema al presentar la concentración de la criticidad de los riesgos por zonas.

Pareto: Al ubicar los valores de frecuencia organizados y mostrar a través de una línea la frecuencia acumulada nos permite mostrar el significado de la frecuencia relativa así como el grado en perspectiva del riesgo del conjunto de amenazas.

Ishikawa (espina de pescado): Nos permite realizar un estudio más profundo de la relación causa efecto y a su vez permite exponer de una manera “masticada” las causas primarias y secundarias de las amenazas.

Grafos: Son muy útiles a la hora de establecer relaciones no siempre implícitas.

Otro de los factores que pueden malograr nuestra intención es el uso de métricas ultra complejas, confusas o que no reflejen realmente la medida del elemento que deseamos evaluar o en el peor de los casos la ausencia de ellas, esto último convierte el informe en un discurso o monologo y podría generar incógnitas más que develarlas.

Lo más importante a la hora de comunicar los resultados es recordar que la audiencia por excelencia a la cual está dirigida tiene limitados conocimientos en el tema y mas que demostrar cuanto sabemos o cuan

profundo fue nuestro análisis nuestra prioridad es ser comprendidos y garantizar que, sin crear pánico innecesario los que nos escuchen lleven más que una noción del estado de la seguridad de nuestro sistema y la verdadera criticidad que esto implica.

3. RESULTADOS Y DISCUSIÓN

El uso del UML para modelar el negocio arrojo como resultado una inadecuación del mapa de procesos definido en la empresa al mostrar este solo 13 mientras que se identificaron 56 procesos simples y otros tantos actores rescatando información relativa a la interacción y flujo de las actividades en la organización. El enfoque de las amenazas como variable estadística permitió una evaluación más clara y precisa del riesgo y se corrigieron errores de evaluaciones de riesgo anteriores donde por desconocimiento de la organización se obviaban riesgos o se le atribuían funciones a activos que en realidad no la poseían. El enfoque de separar a la evaluación los mecanismos de seguridad ha permitido detectar fallas en los procedimientos como en el caso del procedimiento de empleo u optimizar mecanismos de control como en el caso de las incidencias y la trazabilidad del soporte brindado por el grupo de informática. El uso de estas herramientas nos permite establecer las bases de un sistema traceable en todo momento y redunda en una mayor organización y eficacia del sistema de seguridad informática. En el orden económico una evaluación más precisa, correcta o valida de los riesgos operacionales pero además tener en cuenta los riesgos organizacionales nos permiten trazar mejor las estrategias garantizando minimizar las pérdidas y el esfuerzo y dándole un agregado de valor al producto.

En los resultados del análisis de gestión de riesgos se hace importante y casi imprescindible el uso de herramientas tales como los gráficos de Pareto, histogramas y gráficos de dispersión esto y un lenguaje simple y objetivo permitirá a nuestros dirigentes captar la importancia, el estado y les hará involucrarse tempranamente en las labores de seguridad.

4. CONCLUSIONES

Nuestra hipótesis acerca de la importancia de capturar la esencia del contexto de negocio se ve respaldada por los resultados obtenidos.

En este trabajo se logran los siguientes objetivos:

- Reducir la subjetividad en el análisis
- Brindarle un espacio al análisis de los riesgos organizacionales
- Una evaluación pormenorizada de los mecanismos de seguridad
- Mantenerse dentro del marco legal y normativo
- Crear un proceso auditable

Estos objetivos se han alcanzado mediante el uso de reconocidas herramientas utilizadas en el mundo entero y redunda en consolidar el sistema de seguridad informática pero además en brindar un resultado de valor a la organización el permitiría no solo prever los riesgos sino

optimizar el funcionamiento del sistema. . Aun nos queda mucho trecho por andar y en estos momentos nos encontramos realizando mejoras para aplicar en una próxima evaluación de riesgos que nos permita enfocarnos en las causas del problema y los factores de planificación estratégica de manera que se facilite la elaboración de una estrategia de mitigación de riesgos y un plan de continuidad del negocio.

La metodología planteada si bien es capaz de brindar resultados por sí misma no está reñida con la vigente actualmente

5. REFERENCIAS BIBLIOGRÁFICAS

- Villacorta Cavero, A., "Desarrollo de una Auditoria Interna basada en la evaluación de Riesgos" en *Congreso Latinoamericano de Auditoría Interna*, Ciudad de La Habana, 2006
- García, E, "Análisis de Riesgos," en *Congreso Latinoamericano de Auditoria interna*, Quito, 2007.
- Segura, J, "IT Governance and Risk Management" en *Congreso Latinoamericano de Auditoria Interna*, Quito, 2007.
- Corletti, A, Matriz *de Estado de Seguridad* Disponible en: http://www.criptored.upm.es/guiateoria/gt_m292d.htm
- Baker, Neil, "Under one umbrella", *Internal Auditor,* pp 39-43, Agosto 2007
- Shields, G. (2007), *Definitive guide to business service management*. Disponible en: www.realtimepublishers.com
- ISO 27001:2005,International Standard Organization,2005.
- "Gestión de Empresas: Procesos operatives y de gestión" Disponible en: http://www.gestionempresarial.info