LA IMPORTANCIA DE REALIZAR UN ANÁLISIS DE RIESGO EN LAS EMPRESAS

Torres, Cesar
cetorre7@hotmail.com
Universidad Piloto de Colombia

Abstract-*In the System Management Information Security, you must perform adequate risk management that allows to know what are the main vulnerabilities of their information assets and what are the threats that could exploit the vulnerabilities are, likewise may establish preventive measures to ensure standards of safety information. Based on the business need and the huge demand for operations presented in organizations with processes, assets, procedures it is important for organizations to plan, do, assess and act upon the identified risks to minimize negative impacts on its assets.*

Resumen-*En el sistema de gestión de Seguridad de la Información, es necesario realizar una adecuada gestión de riesgos que permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades, así mismo podrá establecer las medidas preventivas que garanticen los niveles de seguridad en su información Con base a la necesidad del negocio y a la enorme demanda de operaciones que se presenta en las organizaciones con los procesos, activos, procedimientos es importante que las organizaciones planifiquen, hagan, valoren y actúen en base a los riesgos identificados para minimizar los impactos negativos sobre sus activos.*

Palabras Clave-*Amenaza, Confidencialidad, Disponibilidad, Impacto, Integridad, Probabilidad, Riesgo, Vulnerabilidad.*

I. INTRODUCCIÓN

En este documento se muestran muchas de las metodologías utilizadas para la gestión de riesgos, parten de un punto común con la identificación de activos de información, es decir todos los recursos involucrados en la gestión de la información que va desde datos, hardware hasta documentos escritos y el recurso humano.

Estos activos de información son los que hacen la identificación de las amenazas o riesgos y sus respectivas vulnerabilidades.

II. ANÁLISIS DE RIESGOS

El análisis de riesgo (también conocido como evaluación de riesgo o PHA por sus siglas en ingles Process Hazards Analysis), es el estudio de las causas de las posibles amenazas, daños y consecuencias que estas puedan producir. [1]

El análisis de riesgos crucial para el desarrollo y operación de un SGSI. En esta fase la organización debe construir lo que será su "modelo de seguridad", una representación de todos sus activos y las dependencias que estos presentan frente a otros elementos que son necesarios para su funcionamiento (edificios, suministros, sistemas informáticos, etc.) y su mapa de amenazas (una hipótesis de todo aquello que pudiera ocurrir y que tuviera un impacto para la organización). [2]

El análisis está basado en identificar los activos a proteger o evaluar. La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.

Los resultados obtenidos del análisis van a permitir aplicar alguno de los métodos para el tratamiento de los riesgos que involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlos, preparar planes para este tratamiento y ejecutarlos.

Día tras día va en aumento la cantidad de casos de incidentes relacionados con la seguridad de los sistemas de información que comprometen los activos de las empresas. Las amenazas siempre han existido, la diferencia es que ahora, el enemigo es más rápido, más difícil de detectar y mucho más atrevido. Es por esto, que toda organización debe estar en alerta y saber implementar sistemas de seguridad basados en un análisis de riesgos para evitar o minimizar las consecuencias no deseadas.

Una amenaza se puede identificar como un evento que puede afectar los activos de información relacionados con el recurso humano, eventos naturales o fallas técnicas. Ejemplos de amenazas pueden ser ataques informáticos externos, errores u omisiones del personal de la empresa, infecciones con malware, terremotos, tormentas eléctricas o sobrecargas en el fluido eléctrico.

Es habitual que dada la poca experiencia que existe en empresas sobre la seguridad que en el segundo ciclo del SGSI se debe revisar por si ha habido cambios.

Se realizan una serie de actividades como son, la identificación de activos, amenazas, estimación de impactos y vulnerabilidades, con todo ello ya se puede calcular el riesgo. Pero éste diagnóstico es válido sólo para ese momento puntual en el tiempo. No es algo estático sino que va a cambiar a lo largo del tiempo, nuevos activos, nuevas amenazas, modificación en la ocurrencia de las amenazas (pensar por ejemplo en el caso del phishing, como una amenaza que ha pasado a ser extremadamente frecuente en este último año). Por lo que cada año la organización debe replantearse su diagnóstico y cuestionarse si tiene nuevos síntomas o si los síntomas detectados han sido ya mitigados y se pueden tratar como otras de las carencias de menor importancia. La mejora continua afecta también al riesgo ya que si los niveles más altos se han solucionado, lo lógico es plantearse para el siguiente año atacar los siguientes. [2]

La gestión del riesgo de la seguridad empieza a ser vista con buenos ojos por otras áreas que se dedican a gestionar el riesgo. Es el caso de las entidades financieras que en virtud a Basilea II deben tratar el riesgo operacional. La tecnología es un riesgo operativo y en algunas organizaciones el área de seguridad ha entrado a formar parte de la gerencia de riesgos, así como ahora el área de seguridad está entrando a formar parte en las empresas del compliance.

La vulnerabilidad es una característica de un activo de información y el cual representa un riesgo para la seguridad de la información. Cuando se materializa una amenaza y hay una vulnerabilidad existe una exposición de algún tipo de pérdida para la empresa. Por ejemplo, el hecho de tener contraseñas débiles en los sistemas y que la red de datos no esté correctamente protegida puede ser aprovechado para los ataques informáticos externos.

Una vez identificadas las amenazas, lo más importante del análisis de riesgos es la identificación de controles ya sea para mitigar la posibilidad de ocurrencia de la amenaza o para mitigar su impacto. Las medidas de control que puede asumir una empresa van a estar relacionadas con el tipo de amenaza y el nivel de exposición que represente para la información corporativa.

Una empresa puede afrontar un riesgo de cuatro formas diferentes, aceptarlo, transferirlo, mitigarlo o evitarlo. Si un riesgo no es lo suficientemente crítico para la empresa, la medida de control puede ser aceptarlo, es decir ser consciente de que el riesgo existe y hacer un monitoreo sobre él, esta opción está relacionada con tomar algún tipo de seguro que reduzca una eventual pérdida. Si el riesgo representa una amenaza importante para la seguridad de la información se puede tomar la decisión de Transferir, esta segunda opción tiene que ver con la implementación de medidas preventivas o correctivas para reducir la posibilidad de ocurrencia, impacto del riesgo o de mitigar el riesgo. Finalmente, si el nivel de riesgo es demasiado alto para que la empresa lo asuma, puede optar por evitar el riesgo, eliminando los activos de información y de paso la actividad asociada.

La gestión de riesgos debe garantizarle a la empresa la tranquilidad de tener identificados sus riesgos y los controles que le van a permitir actuar ante una eventual materialización o simplemente evitar que se presenten. Esta gestión debe mantener el equilibrio entre el costo que tiene una actividad de control, la importancia del activo de información para los procesos de la empresa y el nivel de criticidad del riesgo.

Gracias a www.iso27000.es se ha podido dar con FAIR. Esta aproximación trata de ofrecer las bases fundamentales del proceso, una descripción de los conceptos a utilizar, así como un marco para la realización de análisis de riesgos. Es importante señalar que gran parte del marco FAIR puede utilizarse para reforzar, en lugar de sustituir los procesos de análisis de riesgos basados en metodologías tan conocidas como OCTAVE, MAGERIT, MEHARI. [2]

III. PASOS PARA HACER UN ANÁLISIS DE RIESGO

Siguiendo los pasos siguientes.

1. Identificar escenarios de amenaza.
2. Decidir quién puede ser dañado y como.
3. Evaluar los riesgos y decidir las precauciones.
4. Registrar sus hallazgos e implementarlos.
5. Revisar su análisis y poner al día si es necesario.

Identificar escenarios de amenaza: **Se** deben identificar otras preocupaciones para la organización que están relacionadas con sus activos de información críticos y que no son visibles a primera vista. Se puede utilizar un cuestionario por cada tipo de escenario (técnico, físico o humano), que contiene un conjunto de condiciones y preguntas diseñadas para detallar la identificación de amenazas. [3]

Otra manera de identificar condiciones de riesgo es a través de árboles de amenaza, que son estructuras lógicas para visualizar combinaciones de eventos y que consideran amenazas a través de medios técnicos y físicos, con actores internos o externos, por motivos accidentales o intencionales, que pueden provocar alguna consecuencia como la divulgación, modificación, interrupción o destrucción de un activo de información, como se muestra en la siguiente imagen. [3]

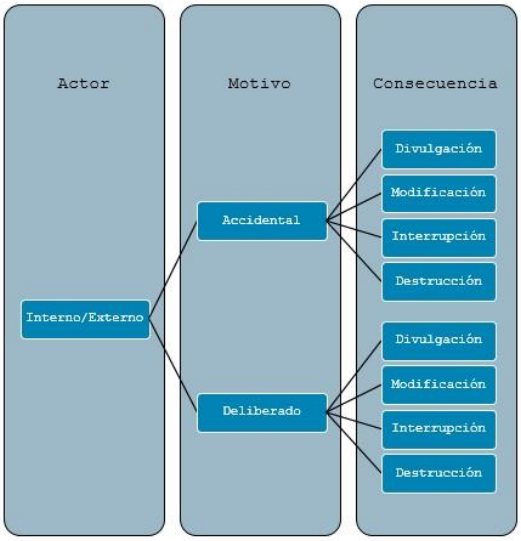

Fig. 1: Imagen Identificar escenarios de amenaza [3]

Otros árboles de amenaza consideran problemas técnicos como defectos de software y hardware, fallas en sistemas o incidentes por códigos maliciosos. También fallas de suministro eléctrico en telecomunicaciones, relacionados con terceros, incluso por desastres naturales que pueden afectar los activos. Es importante mencionar que no todas las combinaciones representan una amenaza real en la organización, por lo que algunas pueden ser descartadas. [3]

Identificar riesgos: El riesgo se puede calcular utilizando la siguiente ecuación.

Riesgo = Amenaza (condición) + Impacto (consecuencia).

Se determina el impacto a la organización si se realiza un escenario de amenaza, la descripción detallada de la manera en que se ve afectada la organización. Para ello se debe tomar como referencia cada uno de los criterios definidos es decir, las áreas de impacto que preocupan a la empresa. [3]

De manera opcional se puede definir la probabilidad realista de la ocurrencia de la amenaza (altamente recomendable). Esta actividad permitirá priorizar los riesgos a tratar y requiere de un conocimiento amplio sobre los problemas de seguridad que ha padecido la organización, por lo que se puede utilizar información estadística como los registros de incidentes. A una probabilidad de ocurrencia alta se asigna un valor de 3, si es media un valor de 2 y una valor de 1 para una probabilidad baja. [3]

Decidir quién puede ser dañado y como: Para cada peligro usted necesita ser claro acerca de quién podría ser dañado, esto le ayudará a identificar el mejor camino para manejar el riesgo.

Recuerde algunos trabajadores tienen particulares requerimientos, como los trabajadores nuevos y jóvenes, gente con capacidades reducidas podrían estar en particular riesgo. Esfuerzos extras serán necesarios para algunos peligros.

Personal de limpieza, visitantes, contratistas personal de mantenimiento etc., quienes podrían no estar en el lugar de trabajo todo el tiempo.

Si usted comparte su lugar de trabajo, usted necesitará pensar acerca de cómo su trabajo afecta a otros presentes, para ello hable con su gente.

Evaluar los riesgos y decidir las precauciones: En este paso se mide de forma cualitativa, el grado en el que la organización es afectada por una amenaza y se calcula una puntuación para cada riesgo de cada activo de información. Para ello se comparan las áreas de impacto de cada categoría, con el escenario de amenaza.

Se debe calcular un puntaje para cada escenario de amenaza generado, en este caso, se considera un incidente de seguridad que se conoce públicamente, por lo que el valor de impacto es alto (correspondiente a un 3). Para cada criterio puede existir más de un área de impacto, por lo que en el cálculo se considera el impacto de mayor valor. Luego se multiplica el valor de impacto del área con la prioridad definida en el paso.

Criterio de evaluación	Prioridad	Valor de área de impacto	Puntuación
Reputación y confianza del cliente	5	Alto (3)	15
Financiera	4	Medio (2)	8
Productividad	3	Bajo (1)	3
Seguridad y salud	2	Bajo (1)	2
Multas y penas legales	1	Alto (3)	3
		Puntaje total	31

Fig. 2: Resultado final valor cuantitativo [3]

El resultado final o puntaje total, es la suma de los productos de la puntuación. El resultado es un valor cuantitativo que puede ir de 0 a 45, a un valor más grande, el impacto será mayor sobre los activos de la empresa.

Seleccionar un enfoque de mitigación: En el último paso, se deben determinar las opciones de tratamiento de riesgos con base en los resultados del análisis, es decir, utilizando los valores de impacto y probabilidad calculados en los pasos anteriores. Este criterio puede variar de una organización a otra, pero en general, se busca mitigar aquellos riesgos que resulten con un valor alto (cercano a 45) y con una probabilidad de ocurrencia alta. [3]

En la metodología seleccionada se puede hacer uso de la matriz de riesgo relativo, un elemento que permite visualizar los riesgos a tratar con base en la probabilidad y el puntaje de riesgo. Se categorizan grupos de escenarios de amenazas para su tratamiento con base en estos resultados, como se muestra en la siguiente imagen. Los riesgos que pertenecen al grupo 1 deberían ser tratados con mayor prioridad.

Matriz de riesgo relativo			
Probabilidad	Puntaje de riesgo		
	30 A 45	16 A 29	0 A 15
Alta	Grupo 1	Grupo 2	Grupo 2
Media	Grupo 2	Grupo 2	Grupo 3
Baja	Grupo 3	Grupo 3	Grupo 4

Fig. 3: Ejemplo de resultado de matriz [3]

Los enfoques de tratamiento para este método son mitigar, postergar, transferir o aceptar. Estas opciones pueden variar de una metodología a otra, aunque generalmente coinciden. Finalmente es conveniente priorizar los riesgos para identificar aquellos que deban tratarse primero.

Con este método, es posible que a partir de criterios cualitativos, se pueda obtener un resultado numérico, es decir un valor cuantitativo, que permite **priorizar los riesgos, con base en un puntaje y su probabilidad de ocurrencia.**

Registrar sus hallazgos e implementarlos: Todos los hallazgos que se generan por medio del análisis de riesgo realizado en la empresa, se debe compartir con todos los involucrados y sus colaboradores. Esto hará la diferencia puesto que usted se está ocupando de su gente y su negocio.

El análisis no tiene que ser perfecto pero debe ser apropiado y suficiente.

Es necesario tener en cuenta lo siguiente.

1. Una apropiada revisión se ha hecho.
2. Se investigó quienes podrían verse afectado.
3. Se evaluaron todos los peligros significativos, teniendo en cuenta el número de personas que podrían ser involucradas.
4. Las preocupaciones son razonables y el riesgo remanente es bajo.
5. Se involucró a todo el personal y/o sus representantes en el proceso.

Si se encontró que es necesario realizar muchas modificaciones y mejoras en las tareas no trate de hacerlas de una vez, elabore un plan de tratamiento el cual lo ayude a, aceptarlo, transferirlo, mitigarlo o evitarlo todos los riesgos identificados.

Un buen plan de acción frecuentemente tiene una mezcla de diferentes cosas tales como.

1. Algunas tareas de bajo costo y fáciles de implementar, quizás como una solución temporaria hasta que una más confiable pueda ser realizada.
2. Soluciones a largo plazo para aquellos riesgos con más probabilidad de accidente y/o daño a la salud.
3. Soluciones a largo plazo para aquellos riesgos que potencialmente tengan la peor consecuencia.
4. Plan de capacitación para empleados sobre los principales riesgos y como ellos pueden ser controlados.
5. Verificaciones regulares para asegurarse que las medidas de control estén en su lugar.
6. Responsabilidades claras de quien lidera la acción y cuando.

Recuerde de priorizar las cosas más importantes primero.

Revisar su análisis y poner al día si es necesario: Pocos lugares de trabajo no se modifican con el tiempo, más tarde o más temprano se traerán nuevos equipos, procesos y procedimientos que podrían generar nuevos peligros, etc. Esto hace necesario por lo tanto, revisar nuevamente. [1]

Cada año, formalmente se debe revisar el análisis, para asegurar la mejora continua. [1]

¿Ha habido cambios?

¿Hay alguna mejora que todavía es necesario hacer?

¿Tienen los trabajadores identificado un problema?

¿Tiene usted aprendido todo sobre accidentes?

Estas son algunas preguntas que nos debemos hacer para asegurarnos que el análisis de riesgo está actualizado. [1]

Cuando usted está trabajando, es muy fácil olvidarse de revisar el análisis de riesgo, hasta que alguna cosa sucede y es demasiado tarde. ¿Entonces porque no hacer el análisis ahora? Deje escrito que la revisión de los riesgos sea un evento anual.

Durante el año, si hay un cambio significativo, entonces no se debe esperar para revisar los riesgos y realizar los ajustes necesarios.

Si es posible, es mucho mejor realizar el análisis de riesgo cuando se están planeando los cambios y no después.

Beneficios de una gestión integral de riesgos.

- Mejor Conocimiento de los riesgos.
- Gestión más eficaz de los riesgos y la crisis.
- Identificación proactiva y aprovechamiento de oportunidades.
- Rápida respuesta a los cambios en el entorno.

- Asignación eficiente de recursos para la gestión de riesgos.
- Establecimiento de base común para comprensión y gestión de riesgos.
- Toma de decisiones más segura.
- Mejor previsión de posibles impactos.
- Mejor orientación de las acciones comerciales.
- Mejor comunicación del valor que crea la compañía.
- Aumento de la credibilidad y confianza.
- Mejora de reputación Corporativa.
- Más probabilidad de éxito en implantación de la estrategia.

Objetivos claves de un proceso de análisis de riesgos.

- Identificar los riesgos que surjan en los planes estratégicos.
- Ayudar a la Gerencia y a Directores (Junta Directiva) a determinar el nivel de riesgo aceptable para la organización.
- Desarrollar actividades para mitigar riesgos, o en su defecto manejarlos en los niveles determinados y aceptados por la organización.
- Desarrollar actividades de monitoreo permanente de forma periódica, a fin de evaluar riesgos y la efectividad de los controles relacionados con ellos.
- Preparar reportes informativos con los resultados del proceso de manejo de riesgos.

Algunos factores de riesgo.

- Rotación de personal.
- Moral de la gerencia y Staff.
- Complejidad de las operaciones.
- Calidad de operaciones manuales.
- Volumen de transacciones diarias.
- Bajos indicadores de rendimiento y/o comportamiento.
- Diseño de programas, desarrollos formales.
- Fecha de la última Auditoría.

Algunos riesgos universales de negocio.

- Costos excesivos.
- Calidad deficiente o inadecuada.
- Pérdida de clientes.
- Pérdidas en ventas.
- Principios inaceptables.
- Errónea información en reportes.
- Destrucción o pérdida de activos.
- Políticas Gerenciales erróneas / decisiones.
- Peligro en la seguridad del público o empleados.
- Fraudes o conflictos de intereses.

Importancia Análisis de Riesgos en las Empresas

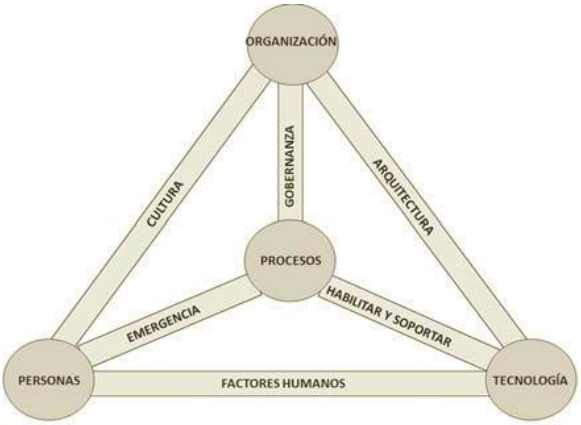

Fig. 4 Modelo de negocio para seguridad de la información. Fuente: Adaptación de: Institute for Critical Information Infrastructure Protection (ICIIP), University of Southern California Marshall School of Business, USA [4]

En la metodología seleccionada como por ejemplo (ISO 27005 vs ISO 31000) al tratar los lineamientos de la gestión de riesgos bajo el esquema presentado de organización integral, permite su inclusión en la gestión de continuidad de negocios como fase de apoyo, en lo respectivo a la identificación de dependencias claves, activos, procesos críticos, amenazas existentes y futuras. Erróneamente la gestión de continuidad es tomada como tratamiento de riesgos pero es importante notar que esta última sirve de soporte para la definición de impactos que puedan producir no disponibilidad en la organización. [4]

Un segundo punto de trabajo se relaciona con los activos de soporte a los procesos analizados. Se analiza hardware, software, recursos humanos y físicos. La finalidad de esta clasificación para el análisis es focalizar el estudio sobre los recursos críticos sin extenderse a activos irrelevantes. [4]

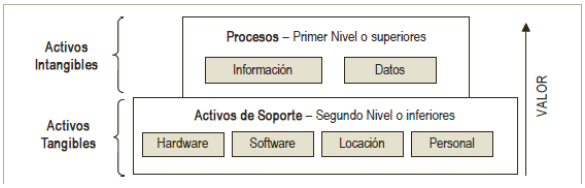

Fig. 5 Activos manejados en la metodología [4]

Para la metodología se utiliza como base el modelo PHVA con la finalidad de establecer un proceso de gestión que se enfoque en la mejora continua siguiendo el esquema presentado a continuación.

PLANIFICAR: Se establecen los objetivos, procesos y procedimientos para el proceso de gestión de riesgos tecnológicos. La finalidad de la planeación es la entrega de resultados acordes con las políticas y objetivos globales de la organización. Así mismo, se establece el plan de comunicaciones y el análisis del

contexto organizacional actual para definir el alcance de la gestión de riesgos tecnológicos. [4]

HACER: Corresponde a la implementación y operación de los controles, procesos y procedimientos (incluye la operación e implementación de las políticas definidas), lo correspondiente a la valoración y tratamiento de los riesgos. [4]

VERIFICAR: Evaluar y medir el desempeño de los procesos contra la política y los objetivos de seguridad e informar sobre los resultados. [4]

ACTUAR: Establecer la política para la gestión de riesgos tecnológicos e implementar los cambios requeridos para la mejora de los procesos. Como parte de las fases verificar y actuar, se incluye el monitoreo y mejora continua, donde se verifican los cambios y el cumplimiento de los indicadores que fueran establecidos desde la planificación. [4]

Como se mencionó anteriormente, la metodología tiene su base en los estándares internacional ISO 31000 e ISO 27005, dado su enfoque en gestión de riesgos y siendo parte de los estándares de la familia ISO fue posible establecer una alineación entre los dos y ajustarlos a la metodología diseñada junto al modelo PHVA (ver Figura 6), a este marco fueron agregadas las mejoras provenientes de otras guías, entre ellas las que se mencionan a continuación. [4]

<table>
<tr><th>PHVA</th><th colspan="3">ISO 27005</th><th>ISO 31000</th></tr>
<tr><td rowspan="11">Planear</td><td colspan="3"></td><td>Mandato y compromiso de la dirección</td></tr>
<tr><td colspan="3">Definir plan de gestión de riesgos</td><td>Diseño del marco de trabajo para gestión riesgos</td></tr>
<tr><td colspan="2">Establecimiento del contexto</td><td rowspan="11">Proceso de gestión del riesgo</td><td>Entender la organización y su contexto</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>Definir responsabilidades</td></tr>
<tr><td>Recursos</td></tr>
<tr><td colspan="2"></td><td>Integración con procesos</td></tr>
<tr><td colspan="2"></td><td>Establecer mecanismo de comunicación</td></tr>
<tr><td>Identificación del riesgo</td><td rowspan="3">Valoración Riesgo</td><td rowspan="5"></td></tr>
<tr><td>Estimación del riesgo</td></tr>
<tr><td>Evaluación del riesgo</td></tr>
<tr><td colspan="2">Desarrollar el plan de tratamiento del riesgo</td></tr>
<tr><td colspan="2">Aceptación del riesgo</td></tr>
<tr><td rowspan="3">Hacer</td><td colspan="2"></td><td>Establecer políticas para la gestión de riesgo</td></tr>
<tr><td colspan="2">Implementar el plan de tratamiento</td><td>Implementación del marco de trabajo para la gestión de riesgos</td><td>Implementar el proceso de gestión de riesgos</td></tr>
<tr><td colspan="2">Implementar plan de comunicación del riesgo</td><td colspan="2"></td></tr>
<tr><td>Verificar</td><td colspan="2">Monitoreo y revisión del riesgo</td><td>Monitoreo y revisión del marco de trabajo</td></tr>
<tr><td>Actuar</td><td colspan="2">Mantener y mejorar el proceso de gestión</td><td>Mejora continua del marco de trabajo</td></tr>
</table>

Fig. 6 Alineación de estándares ISO 31000 e ISO 27005 con modelo PHVA. [4]

Mapa de Calor de Riesgos: El mapa de calor da como resultado de la evaluación de riesgos generada, por medio de la metodología utilizada y por la respectiva valoración de los activos, identificación de las vulnerabilidades y amenazas.

Se representa en formato de matriz con dos ejes. En las ordenadas, la probabilidad de ocurrencia y, en el de las abscisas, el impacto que un riesgo tendría a la hora de materializarse. Cuanto mayor sea tanto la intensidad, como la probabilidad de ocurrencia, tendrá una mayor importancia y debería eliminarse, tratarse o aceptarse en función del apetito de riesgo.

Un mapa de riesgo es una herramienta de visualización de datos para comunicar los riesgos específicos que enfrenta una organización. [6]

El objetivo de un mapa de riesgos es mejorar la comprensión de la organización, aclarar el pensamiento sobre la naturaleza y el impacto de los riesgos, mejorar la organización a través de un modelo de evaluación de riesgos. En una empresa, un mapa de riesgos es a menudo presentado como una matriz. Por ejemplo, la probabilidad de que ocurrirá un riesgo puede ser trazada en el eje X, mientras que el impacto del mismo riesgo se traza en el eje y. los riesgos pueden ser ilustrados con un mapa de calor. [6]

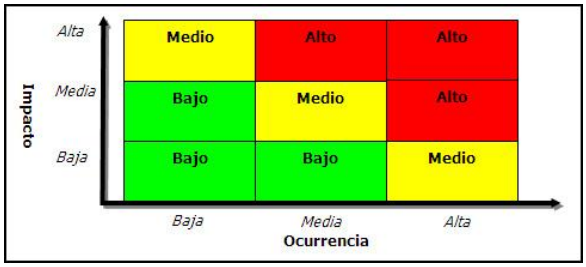

Fig. 6 Mapa de Calor de Riesgos [5]

Durante los últimos años, muchas empresas han adoptado un mapa de riesgo, dentro del marco de gestión del riesgo institucional y puesto en marcha el proceso tomando medidas para identificar y evaluar sus riesgos, pero este ejercicio por una empresa global puede implicar el desarrollo de una lista de riesgos que podrían contarse por cientos. [6]

Una extensa lista de riesgos requiere una buena organización. Un enfoque para la organización de la lista es crear un "registro de riesgos", que permite la categorización, ordenación y clasificación de los riesgos. [6]

IV. CONCLUSIONES

El objetivo de la evaluación de riesgo es identificar y ponderar los riesgos a los cuales los sistemas de información, sus activos o servicios están expuestos, con la finalidad de identificar y seleccionar los controles apropiados.

La gestión de los riesgos tecnológicos es importante dado que las organizaciones al usar tecnología en su actividad diaria y como parte de sus procesos de negocio se encuentran expuestas a este tipo de riesgos; por ello pueden afectar la actividad propia de las mismas y ser fuentes de pérdidas y daños considerables.

Los planes de seguridad deben contemplar crear conciencia a todos los involucrados en las empresas para prevenir los riesgos y buscar una estrategia con el fin de obtener el apoyo de la alta gerencia para poder

cumplir con los objetivos estratégicos de la empresa, evitar en gran medida la generación de incidentes. Por todo esto las empresas deben robustecer su protección físicamente, lógicamente y el factor humano, en estos aspectos se observa la presencia de la tecnología y por esto la información se encuentra expuesta y los activos se deben proteger en gran medida realizando los respectivos análisis de riesgos para poder mitigar la fuga de información.

Para muchas organizaciones la toma de medidas preventivas, que es el principal punto de la gestión de riesgos, y la continuidad de negocios puede pasar como irrelevante, pero su debido cuidado radica la disminución de pérdidas y perjuicios.

REFERENCIAS

[1] http://www.monografias.com/trabajos83/analisis-riesgo/analisis-riesgo.shtml

[2] http://seguridad-de-la-informacion.blogspot.com.co/2008/10/la-importancia-del-anlisis-del-riesgo.html

[3] http://www.welivesecurity.com/la-es/2014/09/30/8-pasos-evaluacion-de-riesgos-2/

[4]http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/4AnalisisycuantificaciondelRiesgo(AR)_es.pdf

[5] http://www.iprofesional.com/notas/124234-Cules-son-las-ventajas-de-una-evaluacin-continua-de-riesgos-y-de-gestin

[6]http://masterenexcel.com/importancia-de-un-mapa-de-riesgo/