LA GESTIÓN DEL RIESGO ACTIVIDAD FUNDAMENTAL PARA LA CONTINUIDAD DEL NEGOCIO

Universidad Piloto de Colombia, Bogotá, Colombia
Guio Suarez, Maycol
mayextream@hotmail.com

Resumen— La actividad de gestión de riesgos se ha convertido en una estrategia fundamental de las organizaciones para optimizar sus operaciones en cuanto al cumplimiento de sus objetivos estratégicos y pensando en la continuidad y disponibilidad de todos los procesos críticos del negocio. Esta gestión realiza ciertas actividades descritas en diversos marcos o guías de referencia de administración de riesgos, las cuales todas apuntan a reducir o minimizar el riesgo para que el impacto generado sea mucho menor.

Abstract- The activity risk management has become a key strategy for organizations to streamline their operations in meeting its strategic objectives and thinking about the continuity and availability of all critical business processes. This makes certain management activities described in different reference frames or guide risk management, all of which aim to reduce or minimize the risk to the impact generated is much lower

Índice de Términos— ISO, continuidad, NIST, Riesgos.

I. INTRODUCCIÓN

La administración de los riesgos, reduce la incertidumbre y facilita el logro de los objetivos de la organización. Este conjunto de procesos, procedimientos y tareas maximizan el buen desempeño empresarial es por esto que las empresas se interesan por conocer el nivel de riesgo en el cual se encuentran y como mediante actividades especificas acordes con sus objetivos estratégicos tratan de reducir los riesgos a un nivel aceptable para la empresa. Es así como la normatividad nacional e internacional desde principios de los años 90, ha definido la importancia de implementar este tipo de herramientas de control que permiten un mejor entendimiento de los procesos, anticiparse a los diferentes tipos de riesgos para con ello gestionar los planes de continuidad y respaldar los procesos críticos del negocio.

Hoy en día existe gran cantidad de guías, normas, marcos, leyes, certificaciones que tratan de la gestión del riesgo bajo la ejecución de distintas actividades unas más que otras pero todas con el objetivo de identificar los riesgos, evaluarlos, clasificarlos y tratarlos, para disminuir el impacto causado por ellos en el caso en que se lleguen a materializar. A continuación se mencionan varias metodologías de gestión de riesgos.

II. CICLO DE ADMINISTRACIÓN DEL RIESGO PROPUESTO POR ISO 27005

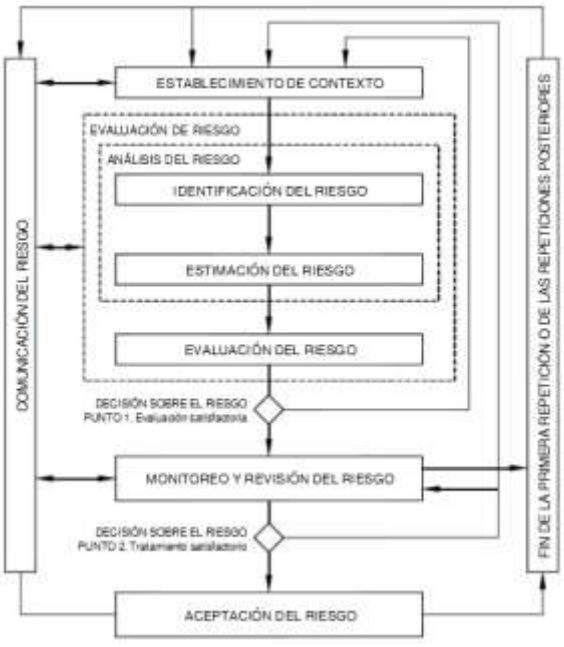

Fig. 1 Proceso de Gestión del Riesgo en la seguridad de la información. [1]

ISO/IEC 27001 e ISO/IEC 27002 definen el riesgo como el potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Dentro de las actividades que propone la norma ISO 27005 de la Figura 1 se menciona el establecer el contexto, que define los parámetros básicos en los cuales se debe manejar el riesgo como el alcance, límites, criterios de evaluación del riesgo, criterios de impacto y criterios de aceptación del riesgo, en los numerales 7.2, 7.3 y 7.4 de la norma ISO 27001 se exponen los elementos del establecimiento de contexto para dar soporte a un SGSI. La identificación de riesgos se realiza a nivel de componente de direccionamiento estratégico, identificando los factores internos o externos a la entidad, que pueden causar una pérdida potencial afectando el logro de los objetivos. En esta actividad se proponen los siguientes pasos que deberían recolectar datos de entrada para la actividad de estimación del riesgo[1]: Identificación de los activos, identificación de amenazas, identificación de controles existentes, identificación de las vulnerabilidades e identificación de las consecuencias.

La estimación del riesgo se realiza de acuerdo a la criticidad de los activos, la amplitud de las vulnerabilidades y los incidentes que han implicado a la organización. Se proponen como metodologías de estimación la cualitativa usando escalas que describen la magnitud y probabilidad de que se materialicen amenazas esta escala puede ser alta, intermedia o baja. La estimación cuantitativa que basa sus resultados en escalas de valores numéricos.

El evaluar el riesgo permite comparar los resultados obtenidos con los criterios definidos para establecer el grado de exposición y así distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

En el tratamiento del riesgo se tiene en cuenta el resultado de la valoración del riesgo y se opta por darle los siguientes tratamientos al riesgo: reducir el riesgo, retener el riesgo, evitar el riesgo y transferir el riesgo.

Al hablar de monitoreo se refiere a asegurar que las acciones se estén llevando a cabo, esta actividad debe estar a cargo de los responsables del proceso y de la oficina de control interno. Ya que los riesgos no son estáticos se deben monitorear los aspectos cambiantes como lo son las amenazas, vulnerabilidades, probabilidades y consecuencias ya que podrían incrementar los riesgos evaluados previamente como bajos.

El aceptar el riesgo es una decisión que deriva del resultado del riesgo residual y que es responsabilidad de los directivos.

Desde el enfoque del SGSI de la norma ISO 27001 las actividades tratadas anteriormente forman parte en el ciclo PHVA de la siguiente manera:

- Planificar: Establecimiento del contexto, valoración del riesgo, planificación del tratamiento del riesgo, aceptación del riesgo.
- Hacer: Implementación del plan de tratamiento del riesgo.
- Verificar: Monitoreo y revisión continuos de los riesgos.
- Actuar: Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información.

III. LA GESTIÓN DEL RIESGO POR DAFP

El departamento administrativo de la función pública plantea su propia guía para el adecuado tratamiento de los riesgos que garanticen el cumplimiento de la misión y los objetivos institucionales de las entidades de la Administración pública[2].

[1] ISO 27005 8.2.1.1 Introducción a la identificación del riesgo

[2] Guía de administración de riesgos DAFP

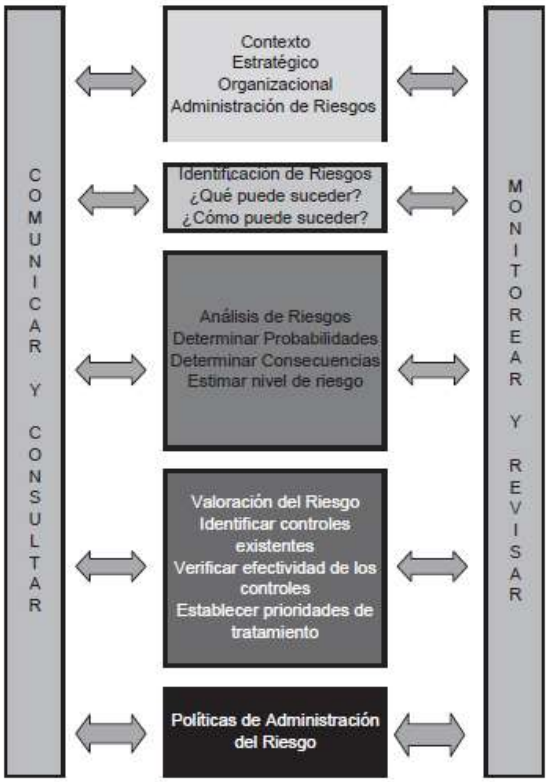

Fig. 2. Guía de administración de riesgos DAFP, proceso de administración del riesgo. [2]

A. Contexto Estratégico

Busca identificar los factores externos e internos que puedan causar riesgos en base al análisis de componentes de direccionamiento estratégico, cultura organizacional, clima laboral, procesos para comprender la misión de la entidad, con esto se logra centrar los objetivos de la administración de riesgo con los objetivos misionales de negocio.

B. Identificación de riesgos

Se platea un formato de identificación de riesgos el cual contiene los campos objetivos nombre del proceso, objetivo del proceso, causas, riesgo, descripción, efectos, consecuencias, campos con los que se busca entender mejor la importancia del riesgo.

C. Clasificación del Riesgo

Se plantea una clasificación y su relación con los procesos que se afectan como lo vemos en la siguiente tabla:

TABLA 1
FORMATO CLASIFICACIÓN DEL RIESGO. [3]

FUENTES DEL RIESGO	PROCESO EN EL QUE IMPACTA				
	Proceso 1	Proceso 2	Proceso 3	Proceso 4	Proceso 5
Estratégico					
Operativo					
Financiero					
Cumplimiento					
Tecnología					

D. Análisis del Riesgo

Busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

E. Valoración del Riesgo

Es el producto de confrontar la evaluación del riesgo con los controles, que se clasifican en preventivos y correctivos, con esta etapa se busca identificar los controles que hay para los riesgos identificados en las etapas anteriores, priorizar los riesgos estableciendo los que mayor impacto causarían en caso de materializarse, elaborar un mapa de riesgos por cada proceso.

F. Políticas de Administración del Riesgo

Fijan los lineamientos para la gestión del riesgo, establecen la posición de la dirección en el proceso y trasmiten las guías de acción todos los funcionarios de la entidad.

IV. MICROSOFT PLANTEA SU GUÍA DE ADMINISTRACIÓN DE RIESGOS

Con el fin de ayudar a sus clientes Microsoft desarrolla la guía de administración de riesgos de seguridad que ayuda a cualquier tipo de cliente a planear, crear y mantener un programa de administración de riesgos de seguridad de forma correcta. Mediante un proceso dividido en cuatro fases, que se muestran en la figura 3. También es

importante tener en cuenta que la administración de riesgos constituye sólo una parte de un programa de gobernanza mayor para la directiva corporativa con el fin de supervisar la empresa y tomar decisiones fundadas [4].

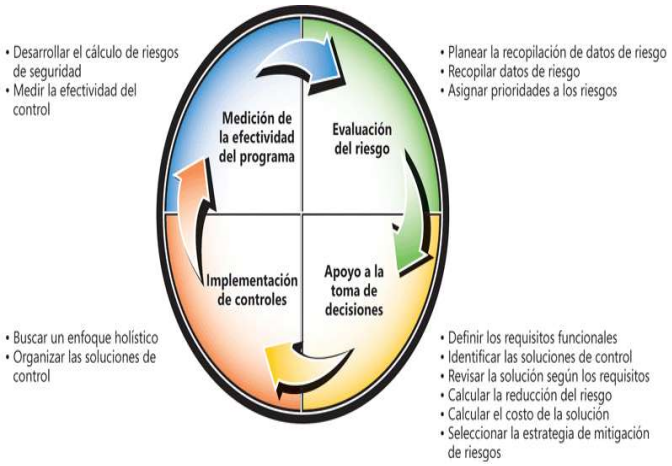

Fig. 3. Proceso de administración de riesgos de seguridad de Microsoft. [5]

La fase de evaluación de riesgos identifica y asigna prioridades a los riesgos en la organización. El proceso de la fase de evaluación de riesgos se divide en tres pasos:

1) Planeamiento: Establece las bases para una evaluación de riesgos correcta.

2) Recopilación de datos facilitados: Consiste en recopilar la información relacionada con riesgos de los participantes de toda la organización, dentro de los datos se recopila información acerca de activos organizativos, descripción de los activos, amenazas de seguridad, vulnerabilidades, entorno actual de controles y controles propuestos.

3) Asignación de Prioridades a Riesgos: Clasificar los riesgos identificados en un proceso coherente.

En la fase de apoyo a la toma de decisiones se determina como afrontar los riesgos del modo mas eficaz y define seis pasos para ello los cuales son: definir los requisitos funcionales, seleccionar las soluciones de control, revisar las soluciones según los requisitos, estimar la reducción del nivel del riesgo que cada control proporciona, estimar los costos a cada solución, seleccionar la estrategia de mitigación de riesgos.

En esta fase también se definirá y seleccionará varios elementos clave de información acerca de cada uno de los riesgos principales que se han identificado durante la fase de evaluación de riesgos mostrando los resultados necesarios para la fase de apoyo a la toma de decisiones.

TABLA 2
RESULTADOS NECESARIOS PARA LA FASE DE APOYO A LA TOMA DE DECISIONES. [6]

Información que se recopilará	Descripción
Decisión acerca de cómo se afrontará cada riesgo	Si se controlará, aceptará, transferirá o evitará cada uno de los riesgos principales
Requisitos funcionales	Declaraciones que describen la funcionalidad necesaria para mitigar el riesgo
Posibles soluciones de control	Lista de controles identificados por los responsables de mitigación y el equipo de administración de riesgos de seguridad que pueden resultar eficaces para mitigar cada riesgo
Reducción de riesgo de cada solución de control	Evaluación de cada solución de control propuestas para determinar en qué medida se reducirá el nivel de riesgo para el activo
Costo estimado de cada solución de control	Todos los costos asociados a la adquisición, implementación, asistencia y medición de cada control propuesto
Lista de soluciones de control que se implementarán	Selección efectuada mediante un análisis de costo-beneficio

La fase de implementación de controles se explica por sí misma: los responsables de mitigación crean y ejecutan planes en función de la lista de soluciones de control surgida durante el proceso de apoyo a la toma de decisiones para mitigar los riesgos identificados en la fase de evaluación del riesgo [7].

En la fase de medición de la efectividad del programa se comprueba periódicamente que los controles implementados durante la fase de implementación de controles estén otorgando realmente el nivel de protección previsto.

V. MAGERIT

Esta metodología es una de las más usadas ya que se encuentra en español, enfatiza en la división de los activos de la organización en varios grupos para poder identificar más riesgos y poder tomar más contramedidas para evitar inconvenientes.

Se basa en tres modelos que son:

1) Submodelo de elementos: Aquí se clasifican los activos, amenazas, vulnerabilidades, impacto, el riesgo y los salvaguardas.

2) Submodelo de eventos: Los elementos del primer modelo se clasifican en dinámico físico, dinámico organizativo, y estático.

3) Submodelo de Procesos: Se compone de cuatro etapas el análisis de riesgo, planificación, gestión de riesgo y selección de salvaguardas [3].

Esta metodología consta de 3 volúmenes: el volumen I explica con detalle toda la metodología, el volumen II proporciona diversos inventarios de utilidad como tipos de activos, dimensiones y criterios de valoración, amenazas, salvaguardas. El volumen III proporciona técnicas a utilizar en las diferentes fases del análisis de riesgos como análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas generales, análisis costo-beneficio, diagramas de flujo, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo, valoración Delphi.

VI. NIST SP 800-30

La NIST[4] ha creado una serie de documentos dedicados a la seguridad de la información la SP 800, en esta serie se incluye una metodología para el análisis y gestión de riesgos de seguridad de la información, alineada y complementaria con el resto de documentos de la serie.

El proceso del análisis del riesgo de la NIST SP 800-30 se resume en el siguiente gráfico:

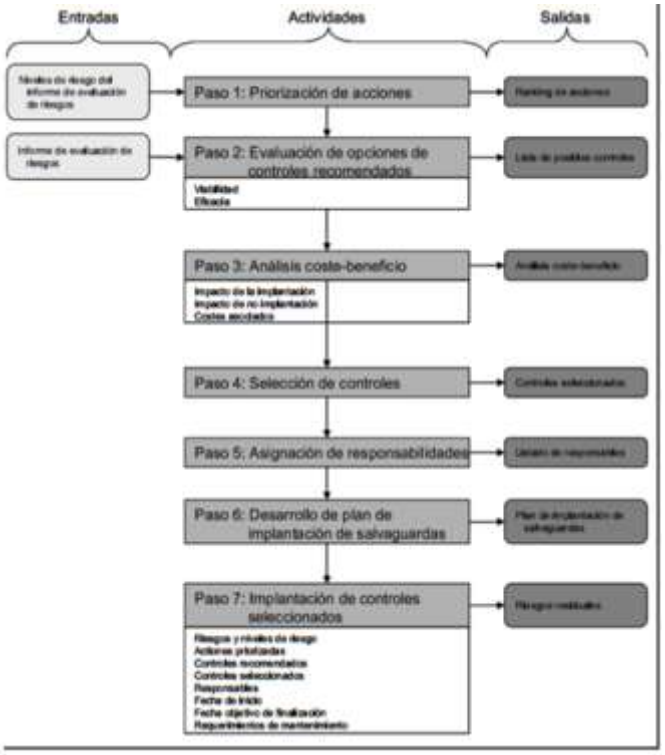

Fig. 4. Organigrama de metodología de mitigación del riesgo. [8]

Esta metodología propone 9 pasos básicos para el análisis del riesgo

- Caracterización del sistema.
- Identificación de amenazas.
- Identificación de vulnerabilidades.
- Control de análisis.
- Determinación del riesgo.
- Análisis de impacto.
- Determinación del riesgo.
- Recomendaciones de control.
- Resultado de la implementación o documentación.

VII. VARIOS MÉTODOS UN MISMO OBJETIVO

Como lo plantea la norma ISO 27005 El propósito de la identificación del riesgo es determinar lo que podría suceder que pueda causar una pérdida

[3] Los controles de las demás metodologías, magerit los define como salvaguardas.
[4] Instituto Nacional de Normas y Tecnología.

potencial, y como tener una idea de cómo, dónde y por qué la pérdida puede ocurrir.[5]

Ya sea estándares como ISO, modelos como COBIT[6], MAGERIT[7], BMIS[8], COSO[9], etc…, guías creadas por entidades del gobierno o grandes empresas como lo es Microsoft buscan el evitar pérdidas o gastos significativos derivados de la exposición al riesgo de las empresas.

Los objetivos básicos o particulares que deberían perseguir cualquier departamento o área de administración de riesgos, que siga alguno de los estándares, modelos o guías existentes se pueden mencionar los siguientes:

- Asegurar el cumplimiento de las políticas definidas por la dirección, en relación con los riesgos.
- Establecer las metodologías de análisis y evaluación de los riesgos.
- Establecer métodos, procedimientos y controles para la administración de riesgos.
- Identificar las fuentes de información adecuadas para medir la magnitud de los riesgos.
- Medir metodológicamente la exposición al riesgo.
- Determinar los niveles de riesgo aceptables de acuerdo con la estructura financiera de la empresa y con las políticas al respecto.
- Establecer, mediante la teoría de escenarios, los posibles cambios o variaciones en las variables que inciden en la exposición al riesgo.
- Elaborar informes constantes sobre la exposición al riesgo.

VIII. EL PORQUÉ DE LA GESTIÓN DEL RIESGO EN UN PLAN DE CONTINUIDAD DE NEGOCIO

El plan de continuidad de negocio BCP, es el conjunto de actividades y estrategias de recuperación definidos que proveen una reanudación oportuna de los procesos que son críticos para el negocio reduciendo el impacto generado ante una contingencia o desastre buscando salvaguardar los intereses de los de los involucrados, la gobernabilidad, la reputación y las actividades de creación de valor de la organización, existen varios estándares y marcos que dentro de su contenido abordan la continuidad de negocio, como lo son: DRII, ISO 22301, COBIT, NIST 800-34. El análisis del riesgo es mencionado en todas las metodologías anteriores como una de las actividades iniciales dentro del plan de continuidad, la gestión del riesgo dentro del plan de continuidad nos permite plantar escenarios coherentes con los riesgos que más probabilidad tienen de presentarse y que generan mayor impacto.

El análisis de impacto al negocio (BIA) y la evaluación de los riesgos suelen ser procesos separados pero deben ser ejecutados simultáneamente o en paralelo. El razonamiento es que la evaluación de impacto en el negocio, sin evaluar el riesgo no proporciona una imagen completa. Podemos pensar en el impacto como una constante; si la interrupción de un sistema crítico tiene un alto impacto (o financiera de otro tipo) en un negocio, no importa lo que hagamos, el impacto de la interrupción real sigue siendo alta. No podemos cambiar el impacto; sólo podemos tratar de evitar la interrupción. [9]

[5] ISO 27005, Pág. 16. Traducción de Maycol Guio Suarez. 07 de mayo de 2013

[6] COBIT es un marco de gobierno de TI y herramientas de apoyo que permite a los administradores para cerrar la brecha entre las necesidades de control, cuestiones técnicas y riesgos de negocio.

[7] Es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

[8] Modelo de negocios para la seguridad de la información creado por ISACA.

[9] El Informe COSO es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de control.

IX. CONCLUSIONES

Es decisión y labor de las empresas estudiar y documentarse sobre los distintos estándares, modelos o guías que tratan de la gestión de riesgos, y del plan de continuidad para proteger sus procesos críticos y asegurar una pronta recuperación frente a una contingencia y que ayuden a garantizar la continuidad y buen prestigio del negocio. Estos modelos se deben escoger e implementar de acuerdo a sus necesidades integrando la solución con sus objetivos estratégicos. El proceso de gestión de riesgos es un poco desconocido dentro del ámbito de las empresas locales, aunque últimamente la mayoría de las entidades del rubro bancario, aseguradoras y financieras la tienen implementadas.

Para que la gestión de riesgos en una entidad sea exitosa no hay que olvidar que una de las etapas más importantes es la de crear conciencia y sensibilizar al personal en la cultura de los riesgos, para que sean ellos mismos quienes puedan controlar y evaluar sus procesos. Para que un plan de concienciación sea exitoso se debe buscar en lo posible el apoyo de la alta gerencia, el involucramiento de las áreas clave, el crear acciones que enfaticen en cómo hacer las cosas mas no que es lo que no hay que hacer, monitorear los resultados del plan mediante indicadores y sobretodo hacer llegar el mensaje de una manera respetuosa y amigable.

Debido a la necesidad que tienen las empresas de proteger las inversiones realizadas en activos informáticos se debe asegurar la continuidad y la confiabilidad de operación de la tecnología al servicio de su empresa.

APÉNDICE

ISACA es la entidad Internacional que emite certificaciones, modelos y referencias de gobierno de seguridad de la información y la cual propone varios modelos a seguir para un gobierno de seguridad de la información.

REFERENCIAS

[1] *Proceso de gestión del riesgo en la seguridad de la información* [En línea]. Disponible en: http://es.scribd.com/doc/124454177/ISO-27005-espanol.

[2] *Proceso de administración del riesgo*. [En línea]. Disponible en : http://portal.dafp.gov.co/form/formularios.retrive_publicaciones?no=558

[3] *Formato clasificación del riesgo*. [En línea]. Disponible en : http://portal.dafp.gov.co/form/formularios.retrive_publicaciones?no=558

[4] *Guía de administración de riesgos*. [En línea]. Disponible en: http://www.microsoft.com/spain/technet/recursos/articulos/srsgch06.mspx.

[5] Proceso de administración de riesgos de seguridad de Microsoft. [En línea] Disponible en: https://www.microsoft.com/spain/technet/recursos/articulos/srsgch03.mspx.

[6] *Resultados necesarios para la fase de apoyo a la toma de decisiones*. [En línea]. Disponible en : https://www.microsoft.com/spain/technet/recursos/articulos/srsgch05.mspx.

[7] Guía de administración de riesgos. [En línea]. Disponible en: https://www.microsoft.com/spain/technet/recursos/articulos/srsgch06.mspx.

[8] Organigrama de la metodología de la gestión del riesgo, Nist Special publication 800-30, 54 páginas (Julio 2002), Traducción de Maycol Guio Suarez, 25 de Julio de 2014.

[9] Revista de seguridad Informática. [En línea]. Disponible en: http://searchdisasterrecovery.techtarget.com/answer/The-difference-between-a-BIA-and-a-risk-analysis-process

Autores

Elaborado por:
Maycol. Guio S.
Especialización Seguridad Informática
Universidad Piloto De Colombia
2014