Análisis y Evaluación de Riesgos en Tecnologías de Información ¿Valen la pena?

Adrián Palma Castillo
Artículo publicado en cuatro partes en la Revista BSecure en el 2008

En este artículo exploraremos los fundamentos del análisis y evaluación de riesgos para continuar con las metodologías y modelos mas reconocidos internacionalmente y por último conocer lo que se requiere para realizar en la vida real un análisis de riesgos tomando en cuenta sus ventajas, desventajas, beneficios y limitaciones. En la actualidad todo mundo habla de Análisis y evaluación de riesgos, el cumplimiento de los marcos regulatorios como Sarbanes Oxley, los lineamientos de la Comisión Nacional Bancaria y de Valores, Basilea II etc., también es requerido por los estándares de la industria como el ISO 27001, y las normativas internas de los grandes corporativos y empresas trasnacionales , pero la realidad es que el enfoque con el cual se realizan estos proyectos no cumplen con el objetivo principal de este análisis que es conocer realmente el nivel de riesgo aceptable con el cual puede vivir una organización, y de esa manera conocer los riesgos y las alternativas que tengo para poder manejarlos (Risk Management) todo esto lo veremos a través de los artículos ya mencionados por lo pronto empecemos por entender que es esto del análisis de riesgos.

Mi primera participación en un proceso de Análisis y Evaluación de Riesgos (AER) en la vida real fue en el año de 1996 cuando trabajaba para una firma internacional, aunque ya contaba con cierto conocimiento teórico de la materia en ese momento entendí dos cosas que marcarían mi vida profesional, la primera es que el AER es el factor crítico de éxito para cualquier proyecto relacionado con la seguridad en Tecnologías de Información (TI) y la segunda es que este tipo de proyectos son muy difíciles de entender, vender y justificar a la alta dirección ya que hablar de riesgos en tecnología es complejo, los resultados son de alguna manera intangibles y el retorno de la inversión es complicado de demostrar, pero una vez que estos son entendidos créanmelo los resultados son de mucha valía para cualquier organización teniendo en cuenta que el AER se ejecuto de forma correcta. El tema me apasiono y me propuse conocer más a fondo de todo lo relacionado con los riesgos en TI desde sus inicios, enfoques (Cuantitativos y Cualitativos), metodologías, modelos, herramientas etc. etc.

El AER inicialmente tuvo un enfoque cuantitativo ya que en ese tiempo los ambientes de procesamiento eran totalmente centralizados y era mucho mas sencillo cuantificar el valor de los activos y la probabilidad de ocurrencia de las amenazas para así poder calcular la perdida en dinero del impacto de la materialización de un riesgo, todo esto estaba basado en formulas y ecuaciones matemáticas. Este tipo de enfoque hoy día desde mi punto de vista es obsoleto e impráctico ya que la dificultad de poder obtener datos precisos de probabilidades de ocurrencia de las amenazas es muy difícil o ¿alguien podría calcular la probabilidad de cuantas veces cometerán errores o acciones indebidas los usuarios? O ¿cual es el valor de un CD con información? y aun en el supuesto caso de que se pudieran obtener ¿cuanto tiempo estaría dispuesta la organización en fondear un proyecto que tardaría meses?

Con el paso del tiempo el AER cambio a un enfoque cualitativo que es el más usado hoy día y que presenta los riesgos de una organización clasificados en altos, medios y bajos, en mi experiencia las organizaciones no requieren saber el 3.1416 es decir la precisión de los valores del riesgo, sino cuales son aquellos riesgos que pudieran poner en peligro la capacidad de operación, servicio o en algunos caso la supervivencia de la organización y contestar la pregunta mas importante ¿que nivel de seguridad requiere mi organización?.

La alta dirección de cualquier organización tiene la responsabilidad de poner atención, atender y facilitar lo necesario para llevar a cabo un AER de su organización (llamado en ingles el “Due Diligence”) este concepto en otros países esta legislado, hoy día en nuestro país en algunos sectores (Financiero, Empresas Trasnacionales) empieza a ser una cuestión de compliance (Cumplimiento) dentro de estas organizaciones pero debemos entender que si este tipo de proyectos no es apoyado por la alta dirección será prácticamente imposible de ser realizado.

.

La causa principal por la que fallan los AER es porque su alcance esta limitado a las áreas de TI y no a las áreas de negocio o funcionales recordemos que la función de TI es totalmente de servicio para dichas áreas, por lo que cuando se trate de mitigar los riesgos tecnológicos estos deben ser los que afecten a las áreas funcionales o de negocio de la organización. Un AER debe completarse en semanas no en meses o años y debe ser eficaz, eficiente y asertivo para que tenga el impacto esperado.

Para ser efectivo, el proceso de análisis y evaluación de riesgos debe ser aceptado como parte del proceso del negocio de la empresa. El profesional de seguridad en Tecnologías de Información (TI) busca asegurar que el proceso de análisis y evaluación apoyen los objetivos del negocio o la misión de la organización. Durante años se ha tratado de concientizar a los profesionales de seguridad y auditoria a entender que la seguridad o los requerimientos de auditoria no es lo que el negocio o la organización necesita. Hay que recordar que parte del éxito de un proceso de análisis y evaluación de riesgos es su aceptación por parte de todo el personal de la organización. Tratar de imponer la seguridad a la alta dirección sin fundamentos puede resultar contraproducente. Un proceso de análisis y evaluación de riesgos efectivo buscara las necesidades reales de la organización e involucrara a los dueños de la información (por lo regular los dueños de los procesos de negocio) para identificar los controles que cumplan sus necesidades.

La mayoría de los enfoques del proceso de análisis de riesgo se basan en el triangulo CID que contiene los 3 principios de seguridad de la información Integridad, Confidencialidad y Disponibilidad.

El proceso de análisis y evaluación de riesgos debe ser alineado para apoyar al negocio o a la misión de la organización. Muchas veces se les informa a los dueños de la información que ciertos controles están siendo implementados debido a que los controles son “requisitos de seguridad” o “requisitos de auditoria” Tal como lo hemos discutido, solo existen requisitos del negocio y/o requisitos de la misión y estos deben de beneficiar realmente a la organización para mitigar los riesgos que podrían poner en peligro la capacidad de operación, servicio y en algunos casos hasta la supervivencia de la organización.

Cada organización tiene que establecer su propio conjunto de requisitos para la protección de sus activos de información (Datos, Hardware, Software, Redes, Sistemas Operativos, Bases de Datos, Aplicaciones, Instalaciones, Personal, Dinero Procesos de Negocio etc., etc.). Esto es comúnmente documentado a través de una política de clasificación de la información. Los controles diferirán dependiendo de la sensibilidad y criticidad del activo de información. Por lo tanto, la meta de un programa de seguridad de la información a lo largo de una empresa y de un proceso de análisis y evaluación de riesgos es determinar el impacto de la materialización de las amenazas en los activos de información basado en:

- Integridad: Se requiere que la información no sea modificada inapropiadamente.
- Confidencialidad: La información es protegida del acceso no autorizado o la divulgación accidental.
- Disponibilidad: los usuarios autorizados pueden acceder a la información cuando lo requieran para realizar su trabajo.

El proceso de clasificar la información necesita estar perfectamente definido, y se necesita implementar una metodología para ayudar a los usuarios a determinar el nivel de clasificación como parte del proceso de análisis y evaluación de riesgos. Para ayudar a dicho proceso, será necesario hacer que los usuarios visualicen todos elementos que dan valor al activo en dicha evaluación.

Estos pueden incluir algunos, todos o más de los siguientes:

- El costo de producir la información
- El valor de la información en el mercado
- El costo de reproducir la información si fuera destruida
- El beneficio que trae la información a la empresa al cumplir los objetivos del negocio o de la misión.

- Las repercusiones para la empresa si la información no esta disponible.
- La ventaja que se le daría a la competencia si pudiera usar, cambiar o destruir la información.
- El costo para la empresa si la información fuera divulgada, alterada o destruida.
- La pérdida de confianza del cliente o la pérdida del cliente si la información no es segura.
- La pérdida de imagen y pérdida de negocio además de sanciones por no tener información segura.

El valor del activo de información debe ser determinado por el dueño de la información, donde la información es creada o es el usuario principal de ese recurso. Esta es una actividad que no puede ser responsabilidad de la función de seguridad de la información o de la función de informática o de auditoria, o de cualquier otra área. Esta es una responsabilidad de los dueños de la información

Las etapas del Análisis y Evaluación de Riesgos.

El proceso de análisis y evaluación de riesgos comúnmente consta de cuatro elementos: los activos de información, las amenazas identificadas, las vulnerabilidades identificadas el nivel de riesgo establecido, y los controles seleccionados.

Activos de Información

¿Qué es entonces un activo de información? Un financiero podría decir que un activo es algo que tiene un valor. Sin embargo, los activos de información físicos o tangibles no son los únicos activos que deben protegerse también tenemos que proteger aquellos activos intangibles como la imagen, la propiedad intelectual, etc., etc.

Identificación de la amenaza

Después de que se ha identificado el activo que necesita ser protegido se deben identificar las amenazas que podrían afectar a los activos involucrados en el análisis y evaluación de riesgos. ¿Entonces que es una amenaza? Es un evento o circunstancia capaz de causar un daño pueden existir un número ilimitado de amenazas que pueden afectar a su organización.

Existen tres fuentes comunes para las amenazas, y pueden ser clasificadas como naturales, humanas o ambientales. Recuerde que la categoría humana esta dividida en dos subcategorías: accidentales y deliberadas. Tal y como hemos mencionado antes, las amenazas humanas deben ser vistas a través de actos deliberados como los ataques por personas maliciosas o empleados a disgusto, o de actos sin intención, como la negligencia o los errores. Recuerde, la motivación esta limitada a las amenazas humanas.

Elementos de amenaza.
Al examinar las amenazas, los expertos identifican tres elementos que están asociados con la amenaza.

- El agente que es el catalizador que realiza la amenaza. El agente puede ser humano, una máquina o la naturaleza.
- El motivo es algo que causa que un agente actúe. Estas acciones pueden ser accidentales o deliberadas.
- Los resultados son el resultado de la amenaza materializada. Durante el proceso de evaluación de riesgo será necesario identificar tantas amenazas como sea posible. Identificar una amenaza es solo la primer parte de la fase del análisis. Será necesario determinar que tan vulnerable es su empresa a esa amenaza.

Determinación del nivel de riesgo

Una vez que hemos identificado las amenazas, será necesario determinar que tan probable es que esa amenaza pueda ocurrir. Al examinar la amenaza existen dos formas claves de evaluar la probabilidad e impacto. El primer método es establecer la probabilidad sin la consideración de los controles existentes. El otro método es examinar el nivel de riesgo tomando en cuenta los controles existentes. Esto permitirá al equipo examinar los controles existentes y establecer un nivel de riesgo basado en que tan eficaces son los controles existentes. La probabilidad a la que es susceptible una organización respecto a una amenaza específica se describe típicamente como alta, media o baja.

Una vez que la probabilidad de que las amenazas ha sido determinada, entonces el Impacto de las amenazas tendrá que evaluarse. Antes de determinar el nivel del impacto, es necesario asegurar que el alcance del análisis y evaluación de riesgos se ha definido claramente (figura1).

Nivel de impacto	Definición
Alto	La perdida de confidencialidad, integridad o disponibilidad podría ser esperada o tener efectos severos en las operaciones organizacionales, activos o individuos. • Degradación severa o perdida de la capacidad de la misión en una extensión y duración que la organización no es capaz de realizar sus funciones primarias. • Resulta en un daño mayor para los activos de la organización. • Resulta en perdidas financieras mayores. • Resulta en daños severos o catastróficos para los individuos involucrando la perdida de la vida o serias amenazas a la vida.
Medio	La perdida de confidencialidad, integridad o disponibilidad podría ser esperada o tener efectos serios en las operaciones organizacionales, activos o individuos. • Degradación significativa en la capacidad de la misión en una extensión y duración que la organización es capaz de realizar sus funciones primarias, pero la efectividad es reducida. • Resulta en un daño significativo para los activos de la organización. • Resulta en perdidas financieras significativas. • Resulta en daños significativos para los individuos pero no en la perdida de la vida o serias amenazas a esta.
Bajo	La perdida de confidencialidad, integridad o disponibilidad podría ser esperada o tener efectos limitados en las operaciones organizacionales, activos o individuos. • Degradación en la capacidad de la misión en una extensión y duración que la organización es capaz de realizar sus funciones primarias, pero la efectividad es reducida. • Resulta en un daño menor para los activos de la organización. • Resulta en perdidas financieras menores. • Resulta en una exposición menor al daño.

Figura 1. Definición del nivel de impacto

Una vez el equipo ha establecido el nivel de probabilidad y el nivel de impacto, podrá asignar un nivel de riesgo. Esto puede hacerse creando una matriz de nivel de riesgo como se muestra en la figura 2.

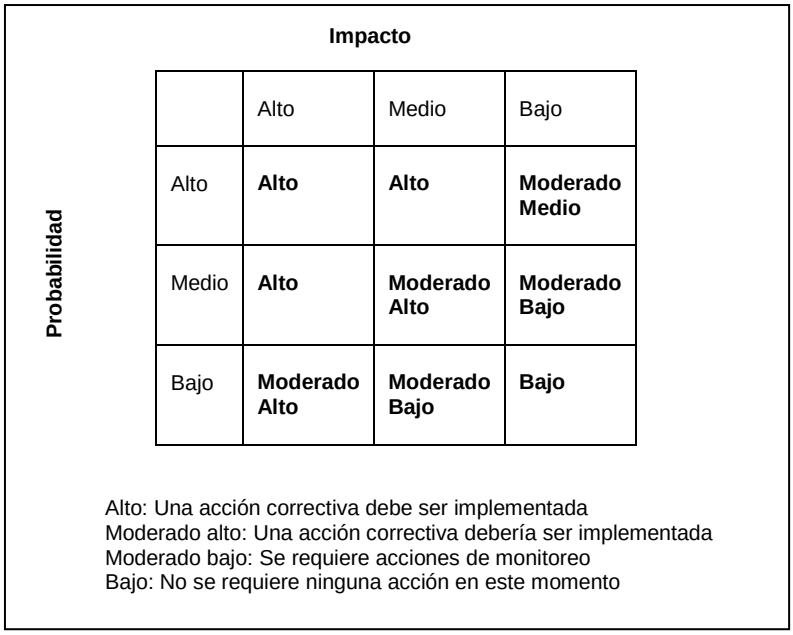

Figura 2. Matriz del nivel de riesgo

Después de que el nivel de riesgo ha sido evaluado, el siguiente paso es preguntarse ¿que se va a hacer con los riesgos? esta etapa es conocida como el manejo o la administración del riesgo (Risk Management) y básicamente hay 3 alternativas, una es **tolerar** el riesgo (no se implementan controles), otra es **transferir** el riesgo (se transfiere el riesgo a un tercero) y la ultima es **mitigar** el riesgo (se implementan controles), esta alternativa es la que tiene un peso mayor en el proceso del AER ya que en esta se buscara que la organización tenga un nivel aceptable de riesgos. Por consiguiente, será importante identificar tantos controles como sea posible. En esta etapa se requiere la participación de especialistas de seguridad. Al seleccionar cualquier tipo de control será necesario medir el impacto operacional para la organización. Cada control tendrá un impacto de alguna manera. El costo de los controles debe ser analizado y evaluado detalladamente, Una buena regla de dedo es evaluar si el control es más caro que el activo que va a proteger no se debe implementar.

Durante esta etapa se podrá determinarán si se requieren controles de seguridad basados en algún estándar, como El Código de Prácticas para la Gestión de la Seguridad de la Información (ISO/IEC 17799-1, BS7799-2 hasta Diciembre del 2005 o el ISO27001 a partir del 2006), la ley Gramm Leach Bliley (GLBA) o la ley Sarbanes Oxley (SOX)

Análisis Costo-Beneficio

Después de identificar todos los controles posibles y evaluar su viabilidad y efectividad se debe realizar un análisis costo-beneficio. Este proceso debe ser realizado para cada control, para determinar si el control recomendado es apropiado para la organización. Un análisis de costo-beneficio debe determinar el impacto de implementar y después determinar el impacto de no implementarlo. Uno de los costos a largo plazo de cualquier control es el requerimiento de mantener su efectividad. Al realizar un análisis de costo-beneficio es necesario considerar el costo de implementación basado en los siguientes factores:

- Costo de implementación incluyendo la inversión inicial para el software y hardware, como mantenimientos soporte etc. etc.
- Reducción de efectividad operacional
- Implementación de políticas adicionales y procedimientos para apoyar a los controles
- El costo de la capacitación que apoye al personal a mantener la efectividad del control.

Prácticamente ningún activo o actividad esta libre de riesgo, y no todos los controles implementados pueden eliminar el riesgo, el propósito de manejar los riesgos es tener a la organización con el nivel de seguridad que realmente requiere para tener un nivel aceptable de riesgo y que la operación, la capacidad de servicio no se vean afectadas por la implementación de controles además de que la inversión sea razonable y que no se hagan inversiones cuantiosas e innecesarias. Un programa de seguridad que tiene como su meta el 100% de seguridad causara que la organización tenga 0% de productividad, teniendo en cuenta que ningún control mitigara el 100% del riesgo en ninguna situación.

Pasos para ejecutar un proyecto de análisis y evaluación de riesgos

Paso 1: Desarrollar una declaración del alcance

El hablar de análisis y evaluación de riesgos es un tópico difícil de entender por su naturaleza y muy importante que la gente de negocio entienda los beneficios y ventajas de ejecutar un proyecto de análisis de riesgos y por el contrario y las perdidas y desventajas de no hacerlo bien.

Para realizar exitosamente cualquier tipo de proyecto es necesario definir perfectamente el alcance para dicho proyecto, en un análisis y evaluación de riesgos no es la excepción. El saber y entender perfectamente el alcance del análisis de riesgos es un factor crítico de éxito. Hoy día este alcance en la mayoría de las organizaciones esta orientado a la función de TI comprendiendo las redes, sistemas operativos alguna que otra aplicación y base de datos, pero difícilmente se hace a un proceso core o critico de la organización y mucho menos a toda la organización. En mi experiencia y al haber realizado más de 15 proyectos de esta naturaleza la mayoría de ellos con un alcance de toda la organización les puedo compartir que se obtienen mejores resultados teniendo un alcance organizacional ya sea de uno o varios procesos o teniendo como alcance toda la organización aunque esto es la mayoría de las veces muy difícil de vender por todos los problemas relacionados a la seguridad (La percepción de que la seguridad es un mal necesario que no aporta ningún valor real y tangible a la organización etc.)

Al desarrollar la declaración del alcance, es de suma importancia identificar al patrocinador o sponsor del proyecto que por lo general es el nivel más alto jerárquicamente del alcance del análisis de riesgos.

La declaración del alcance debe buscar objetivos relacionados con el impacto de las amenazas que afectan la integridad, confidencialidad, y disponibilidad de la información, que en este caso es el activo mas importante de una organización y que dicha información es procesada por aplicaciones y soportadas por la infraestructura tecnológica (Bases de datos, sistemas operativos, redes etc.). Hay que considerar los retos de seguridad de la información que enfrenta su organización, y alinearlos a dichos impactos para definir los objetivos del proyecto tomando en consideración las preocupaciones acerca de cómo estos impactan los objetivos o la misión de la organización ya que la seguridad debe estar siempre alineada a los requerimientos de la organización.

Paso 2: Definición del equipo del proyecto

Es esencial formar un equipo interdisciplinario, entre mas personas conozcan las distintas funciones y procesos de la organización será mas enriquecedor. Otro factor crítico de éxito es el grado de conocimiento y la experiencia de los responsables para ejecutar este tipo de proyectos no solo en la metodología sino en todo el ambiente la metodología siempre nos dirá el QUE mas no el COMO aunado a todas las cuestiones externas (cotos de poder, grillas, apatías, alineaciones con los jefes en cuestión de criterios etc.) Recordemos que en un proyecto de análisis de riesgos uno de los principales problemas a los que nos enfrentamos es el consenso de los participantes .Muchos profesionales de seguridad de Información intentan ejecutar el análisis de riesgo solos o solamente con otros miembros del grupo de seguridad. Para ser eficaz, el proceso de evaluación de riesgo debe tener representantes de todos los

departamentos y áreas que tienen un interés conferido o concentrado en el alcance del proyecto.

El dueño del proceso del negocio y/o funcional y los usuarios son los miembros más importantes de este equipo. Será su conocimiento y especialización lo que nosotros querremos obtener para identificar las principales amenazas. Será responsabilidad del dueño del proceso funcional o de negocio tomar la última decisión en lo que respecta a implementar controles o no (hablaremos de esto más a detalle en la cuarta entrega).

Paso 3: Identifique las Amenazas

Los miembros del equipo de análisis y evaluación del riesgo determinarán qué amenazas podrían afectar al proceso o a la organización. Esto puede hacerse de maneras diferentes. Una manera es proporcionar una lista de amenazas, muchas metodologías o normas como el BS7799-3 cuentan con un set de estas. Un problema es que la mayoría de estas son amenazas orientas a la parte técnica y no a las de un proceso u organización especifica. Otro problema con estas listas de amenazas es que podría generarse la falsa idea de creer haber identificado todas las amenazas posibles y esta apreciación no es correcta en ningún sentido es conocido que lo que realmente hace complejo la ejecución de estos proyectos son precisamente las amenazas. Al usar una lista, hay que asegurarse de conseguir que el equipo intente determinar otras amenazas que puedan ser apropiadas para esto podemos hacer una sesión de lluvia de ideas. La clave de la lluvia de ideas es obtener tantas amenazas como sea posible para cada categoría (integridad, confidencialidad y disponibilidad).

Una vez que la lista está completa, el equipo tendrá que desarrollar las definiciones apropiadas para cada amenaza es muy importante que todos los integrantes del equipo estén totalmente homogenizados en la definición de las amenazas. Aunque esto puede consumir mucho tiempo, nos podrá servir para futuros proyectos de análisis de riesgos. Será necesario crear una lista de definiciones de amenazas. Un ejemplo de una lista típica de definiciones de amenazas se muestra en la figura 3.

Origen de la amenaza	*Amenaza*	*Definición*
Natural		
	Terremoto	Un movimiento de la corteza de la tierra, siendo el resultado de ondas en la tierra provocadas por la falla de las rocas o por la actividad volcánica.
	Huracán	El nombre para un ciclón tropical con vientos sostenidos de 74 MPH (65 nudos) o más en el Océano Atlántico Norte, Mar Caribe, Golfo de México, y Océano Pacífico Norte oriental..
	Tormenta de nieve	Una condición de tiempo severa caracterizada por la caída de precipitación helada. Una tormenta tal forma un glaseado en los objetos, creando condiciones de viaje riesgosas y problemas en los servicios públicos.
	Relámpago	Una descarga visible de electricidad producida en respuesta al aumento de electricidad potencial entre una nube y la tierra, entre las nubes, o dentro de una sola nube, o entre una nube y el aire circundante.
	Marea	El aumento en la altura del agua de mar del nivel que normalmente tendría si no hubiera ninguna tormenta. Aunque las olas más fuertes son asociadas con los huracanes, los sistemas de baja presión aun más pequeños pueden causar un aumento ligero en el nivel del mar si el viento y su acarreo simplemente es correcto, este es estima substrayendo la marea astronómica normal de la marea de la tormenta observada.
	Tornado	Una columna de aire girando violentamente extendiéndose entre una nube conectiva y la superficie de la tierra. Es el más destructivo de todos los fenómenos atmosféricos en la escala de tormenta. Ellos pueden ocurrir en cualquier parte en el mundo dándosele las condiciones apropiadas,
Ambiental		
	Falla eléctrica	Una fluctuación momentánea en la fuente de poder eléctrica, que consiste de un incremento de voltaje (cresta), caída de voltaje, o interrupciones de menos de una media hora.

	Interrupción eléctrica	Una ruptura a largo plazo en la fuente de poder eléctrica, normalmente mayor que media hora.
	Emanación	La emanación inadvertida o transmisión de señales de datos de los componentes de computadoras, periféricos de la computadora.
	Incendio	Una conflagración que afecta los sistemas de información a través del calor, humo, o daño de los agentes de supresión. Esta categoría de amenaza puede dividirse en menor, mayor y catastrófico.
	Falla del hardware	Falla de un componente tecnológico suficiente para causar retrasos en el procesamiento o en pérdidas monetarias para la organización.
	Errores del software	Cualquier dato extraño o erróneo en el sistema operativo o en el programa de las aplicaciones que produce errores de procesamiento o retrasos en el procesamiento
	Interrupción de las telecomunicaciones	Cualquier falla de la unidad de comunicaciones o de un componente suficiente para causar interrupciones en los datos que se transfieren vía telecomunicación entre las terminales de la computadora, los procesadores remotos o distribuidos, y la instalación del host de la computadora.
Humana - deliberate		
	Alteración de los datos	La modificación intencional, inserción, o borrado de datos, ya sea por los usuarios autorizados o no autorizados, que compromete el proceso de auditoria, la recuperación, la disponibilidad, la confidencialidad, o la integridad de la información producida, procesada o almacenada por los sistemas de procesamiento de la información.
	Alteración del software	La modificación intencional, inserción, o borrado del sistema operativo o de las aplicaciones, ya sea por un usuario autorizado o no que compromete el proceso de la auditoria, la eficiencia, la recuperación, la disponibilidad, la confidencialidad, o la integridad de la información, de las aplicaciones.
	Amenaza de bomba	Una notificación de la existencia de un dispositivo explosivo en una instalación, sea verdadera o no.
	Revelación	La divulgación intencional no autorizada de la información patentada, clasificada, sensitiva, confidencial de la organización o personal
	Sabotaje de los empleados	Una acción deliberada tomada por un empleado, un grupo de empleados, no empleado(s) junto con un empleado (s) para la no operación de la organización.
	Fraude	Un manipulación no autorizada y deliberada del hardware, software, o de la información con la intención de una ganancia financiera para el perpetrador.
	Huelga	Una acción de los empleados organizada (sindical o no, legal o no) diseñada para detener la operación de la organización. Estas huelgas pueden categorizarse como prácticas de labor injusta, huelgas económicas etc.
	Robo	La apropiación no autorizada de información, hardware, software, medios de comunicación etc.
	Uso sin autorización	Un uso no autorizado de equipo de cómputo o de programas. Los ejemplos de esto incluyen el funcionamiento de programas personales como los juegos, inventarios, y navegación en otros archivos.
	Vandalismo	La destrucción malévola y sin motivo o destrozo de la propiedad.
Humana-accidental		
	Alteración de datos	La modificación accidental, inserción, o borrado de datos o información almacenada en las bases de datos.
		La modificación accidental, inserción, o borrado de sistemas operativos o

	Alteración de software	aplicaciones o piezas de código.
	Revelación	La liberación accidental de la información sensitiva , patentada, clasificada, confidencial para la organización o información del personal
	Errores de usuarios o de administradores de tecnología	Un acto accidental, impropio, o de alguna u otra forma mal seleccionado por un empleado que produce retrasos de procesamiento, daños a los equipos, pérdida de datos, o modificación de los datos.

Figura 3 Lista de definiciones de amenazas

Paso 4: Priorice las Amenazas

Uno de los pasos mas importantes en un análisis de riesgos es la priorización de las amenazas las cuales podremos trabajar en una matriz como la que se presenta en la Tabla 1.Los participantes del proyecto de análisis determinarán cual será la frecuencia de las amenazas. Dado que ésta es una evaluación de riesgo cualitativo, las frecuencias se expresan entre probabilidades de baja frecuencia a alta frecuencia y puede dársele un valor numérico aplicando los factores listados en Tabla 2.

Amenaza	*Frecuencia de la amenaza*	*Impacto de la amenaza*	*Factor de riesgo*

Tabla1. Priorización de amenazas

Cada persona ingresará el valor que su experiencia le diga o si hay datos sobre esas amenazas. Si el miembro del equipo no tiene ningún conocimiento de alguna frecuencia entonces dejara el espacio del campo en blanco y continuaría con la siguiente amenaza. Será necesario establecer perfectamente lo que cada significa cada categoría para que los miembros del equipo trabajen con las mismas definiciones. Un ejemplo sería la tabla 3.

Baja	***De baja a media***	***Media***	***De media a alta***	***Alta***
1	2	3	4	5

Tabla 2. Asignación numérica a las amenazas

Los miembros pueden hacer esta tarea independientemente y entonces promediar los resultados, o cada equipo si es que así se trabaja puede repasar cada amenaza en conjunto al mismo tiempo y llegar a un acuerdo general.

Factor de probabilidad	*Definición*
Bajo	Es extremadamente poco probable que esa amenaza ocurra durante los próximos 12 meses
De bajo a medio	Es poco probable que esa amenaza ocurra durante los próximos 12 meses
Medio	Es posible que esa amenaza ocurra durante los próximos 12 meses
De medio a alto	Es probable que esa amenaza ocurra durante los próximos 12 meses
Alto	Es altamente probable que esa amenaza ocurra durante los próximos 12 meses

Tabla 3. Ejemplo de definición de factor de probabilidad

Una vez que la frecuencia de la amenaza ha sido determinada, esas figuras se graban en la columna de "Frecuencia de la Amenaza", como se muestra en la tabla 4.

Amenaza	*Frecuencia de la amenaza*	*Impacto de la amenaza*	*Factor de riesgo*
Interrupción eléctrica	5		
Revelación deliberada	3		
Fraude	4		
Error de ingreso de usuario	5		

Tabla 4. Ejemplo de frecuencia de la amenaza

Paso 5: El Impacto de la amenaza

El siguiente paso es determinar el impacto de la amenaza, los miembros del equipo tendrán que estimar el impacto de pérdida si la amenaza se llegara a materializarse en los activos definidos en el alcance; un ejemplo es la tabla 5. Para hacer más asertivos y completos los resultados, el equipo tendrá que decidir antes de la revisión del impacto si se tomaran en cuenta controles o no, la segunda opción es la más utilizada.

Baja	***De baja a media***	***Media***	***De media a alta***	***Alta***
1	2	3	4	5

Tabla 5. Ejemplo de impacto de pérdida.

El equipo revisara cada amenaza como lo hizo en el paso anterior. Cada miembro del equipo tomara su experiencia o datos estadísticos según sea el caso si hay datos sobre esas amenazas. Si el miembro del equipo no tiene ningún conocimiento o idea del impacto entonces dejara el espacio del campo en blanco y continuaría con la siguiente amenaza. Será necesario establecer perfectamente lo que significa cada categoría para que los miembros del equipo trabajen con las mismas definiciones. Un ejemplo se presenta en la tabla 6. De igual manera como en el paso anterior Los miembros pueden hacer esta tarea independientemente y entonces promediar los resultados, o cada equipo si es que así se trabaja puede repasar cada amenaza en conjunto al mismo tiempo y llegar a un acuerdo general.

Factor de impacto	*Definición*
Bajo	Un grupo pequeño o departamento afectado; impacto pequeño o sin impacto para los procedimientos del negocio
De bajo a medio	Uno o mas departamentos afectados, ligero retraso par cumplir los objetivos de la misión
Medio	Dos o mas departamentos o unidades de negocio afectadas, retraso de cuatro a seis horas para cumplir los objetivos de la misión
De medio a alto	Dos o mas unidades comerciales afectadas, retraso de uno o dos días para cumplir los objetivos de la misión
Alto	La misión entera de la empresa es afectada

Tabla 6. Ejemplo definición categorías de amenazas

Amenaza	*Frecuencia de la amenaza*	*Impacto de la amenaza*	*Factor de riesgo*
Interrupción eléctrica	5	2	
Revelación deliberada	3	3	
Fraude	4	3	
Error de ingreso de usuario	5	2	

Tabla 7. Ejemplo de asignación de impacto de la amenaza

Paso 6: La Determinación del Factor de riesgo

Durante este paso, el equipo utilizara la frecuencia de la amenaza y su impacto para valorar el factor de riesgo. Los factores de riesgo irán en una escala de un 2 (bajo) a un 10 (alto) algo que es importante considerar es que se debe de lograr un consenso real por parte de los participantes del equipo (Algo de lo mas difícil de lograr en este tipo de proyectos) como ejemplo tenemos la Tabla 8.

Después de que todos los factores de riesgo han sido calculados, el equipo tendrá que identificar posibles controles para cualquier amenaza que obtuvo un factor de riesgo de 6 o superior.

Ninguna empresa tiene los recursos suficientes para examinar todos los activos para calcular sus factores de riesgo. Por consiguiente, será necesario determinar acciones a seguir para factores de riesgo evaluados entre 4 o 5 se deberán monitorear de una manera regular para asegurar que el factor de riesgo no suba a un nivel inaceptable como es el caso de 6 en adelante. Las amenazas con un factor de riesgo de 3 o debajo no requerirán una acción en ese momento.

Amenaza	*Frecuencia de la amenaza*	*Impacto de la amenaza*	*Factor de riesgo*
Interrupción eléctrica	5	2	7
Revelación deliberada	3	3	6
Fraude	4	3	7
Error de ingreso de usuario	5	2	7

Tabla 8. Ejemplo de asignación de factor de riesgo

Paso 7: Identificación de Controles

En este paso, el equipo analizará las amenazas identificadas con un factor de riesgo alto y seleccionará los controles técnicos, administrativos, y operacionales que ofrecerán un nivel rentable y aceptable de protección a los activos. El modelo para los objetivos de protección de la información que ha sido establecido consiste de cuatro capas: la anulación, la convicción, la detección, y la recuperación:

- Los controles de evitación son controles proactivos que intentan minimizar el riesgo de intrusiones accidentales o intencionales.
- Los controles de aseguramiento son las herramientas y estrategias empleadas para asegurar la efectividad continua de los controles existentes.
- Los controles de detección son las técnicas y programas usados para asegurar la detección temprana, la intercepción, y la respuesta a las brechas de seguridad.
- Los controles de recuperación son servicios de planeación y recuperación para restaurar un ambiente seguro rápidamente e investigar la fuente de las brechas de seguridad.

El equipo debe concentrarse en los controles que permitirán que la misión de la empresa funcione proporcionando un nivel adecuado de protección. Puede ser adecuado establecer una lista de posibles controles en cada una de las capas que ayudarán a la organización a cumplir sus objetivos. Algunos ejemplos de controles se encuentran en la tabla 9.

Además de los controles discutidos antes, algunas amenazas podrían requerir un resguardo físico o alguna combinación de controles. El equipo considerará los controles adicionales y determinarán el costo de implementar y mantener los controles propuestos.

Categoría de control	
Evitación	Cifrado y autenticación
	Arquitectura de la seguridad del sistema
	Proceso de análisis de riesgo
	Programa de awareness de la información
	Programa de la seguridad de la información
	Prevención de interrupciones
	Políticas, estándares, guías y procedimientos
	Infraestructura llave publica
	Arquitectura de aplicaciones seguras
	Comunicaciones seguras
Aseguramiento	Revisión de la seguridad de las aplicaciones
	Pruebas estándares
	Pruebas de penetración
	Escaneo de la seguridad perimetral
	Análisis de vulnerabilidades
Detección	Detección de intrusos
	Monitoreo de ataques remotos
Recuperación	Planeación de continuidad del negocio
	Análisis del impacto del negocio
	Planeación del manejo de crisis
	Planeación de recuperación de desastres
	Procedimientos de respuesta a incidentes
	Computo forense

Tabla 9. Ejemplo de asignación de controles

Es importante listar todos los controles considerados y clasificarlos como se muestra en la tabla 10. Esto permitirá a la dirección ver lo que fue considerado y lo que el equipo está recomendando como un control adecuado y rentable. También es importante conocer que un control puede reducir la exposición de riesgo de más de una amenaza, aumentando así su costo-beneficio.

Amenaza	*Frecuencia de la amenaza*	*Impacto de la amenaza*	*Factor de riesgo*	*Posible control*	*Costo del control*
Interrupción eléctrica	5	2	7	Sistema de suministro de energía sin interrupción (UPS)	$ 38 000
				Supresores de variaciones de voltaje	$ 25 por maquina
Revelación deliberada	3	3	6	Políticas para el manejo de información	200 horas del staff de seguridad para desarrollarlas
				Programa de awareness del usuario	20 horas para desarrollar la presentación, 1 hora por cada empleado que asista
Fraude	4	3	7	Listas de control de acceso	Instalación de software
				Registros de auditoria	La capacidad existente con el sistema para bitácoras
Error de ingreso de datos por usuarios	5	2	7	Controles de edición y validación	8 horas adicionales de programación por aplicación

Tabla 10. Ejemplo de clasificación de controles