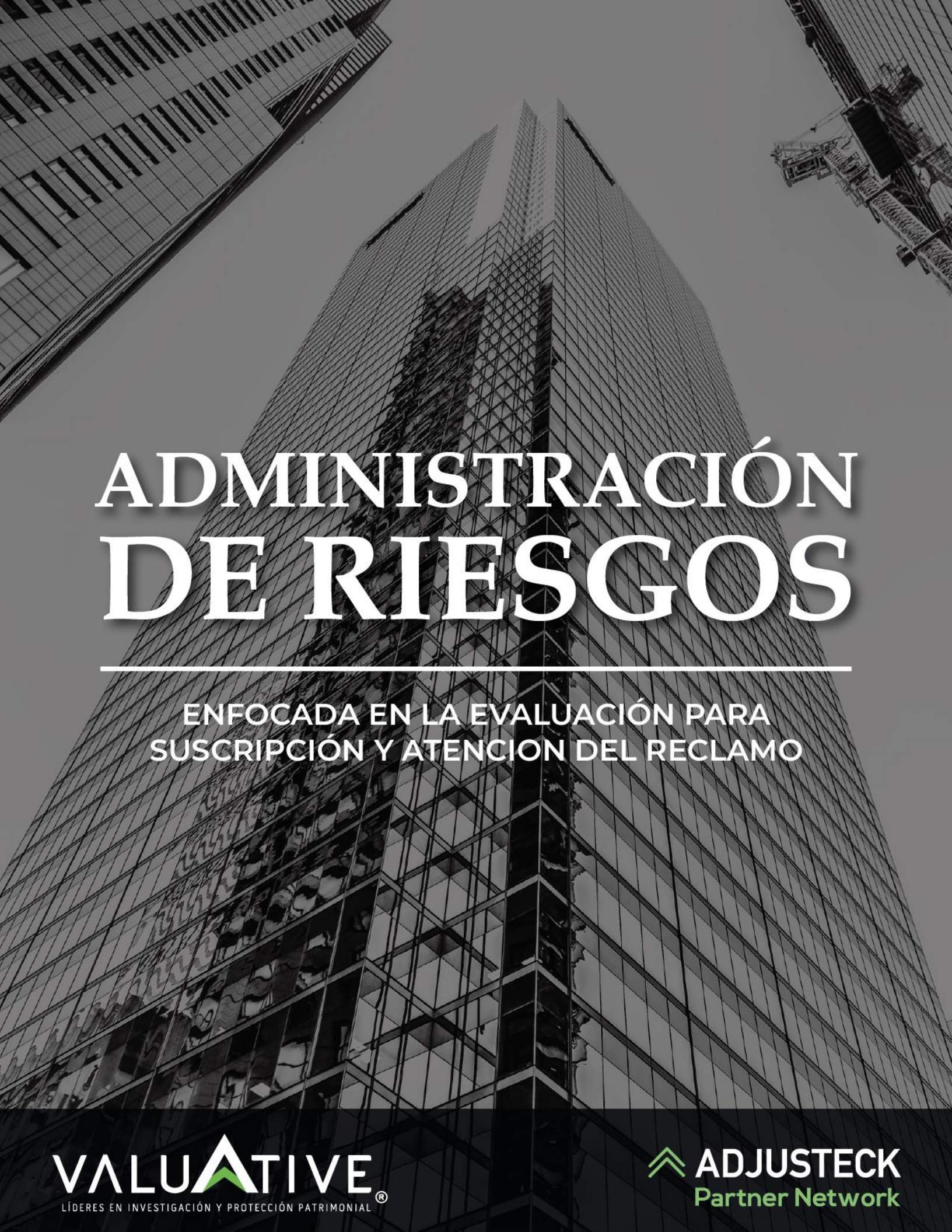

# ADMINISTRACIÓN DE RIESGOS

## ENFOCADA EN LA EVALUACIÓN PARA SUSCRIPCIÓN Y ATENCION DEL RECLAMO

VALUATIVE®
LÍDERES EN INVESTIGACIÓN Y PROTECCIÓN PATRIMONIAL

ADJUSTECK
Partner Network

# ADMINISTRACION DE RIESGOS ENFOCADA EN LA EVALUACION PARA SUSCRIPCION Y ATENCION DEL RECLAMO

## ENTENDIENDO LOS PROCEDIMIENTOS HERRAMIENTAS UTILES EN LA ADMINISTRACION DEL RIESGO DE ATENCION Y DESARROLLO DE LA OPERACION



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

**DEBEMOS CONSIDERAR QUE LA EVALUACION DE RIESGOS SIEMPRE DEBE IR EN DOS DIRECCIONES: DE UNA PARTE LA QUE UNA ASEGURADORA DEBE EJERCER SOBRE SI MISMA Y SUS PROPIOS PROCESOS INTERNOS Y DE LA OTRA, AQUELLA APLICADA A LA PROTECCION EJERCIDA POR SUS CLIENTES ASEGURADOS SOBRE LA PREVENCION Y CONTROL DE SUS EXPOSICIONES A PERDIDA.**

## PRÁCTICAS RECOMENDADAS PARA LA EVALUACIÓN DE RIESGOS EN COMPAÑÍAS DE SEGUROS Y SUS ACTIVIDADES ASOCIADAS

En General, aunque que se piense que las palabras "evaluar" y "analizar" son intercambiables, no son lo mismo en el mundo de la gestión de riesgos.

Una evaluación de riesgos es una evaluación de todos los riesgos potenciales para la capacidad de una organización para hacer negocios. Estos incluyen los riesgos del proyecto, los riesgos funcionales, los riesgos empresariales, los riesgos inherentes y los riesgos de control.

Para las compañías de seguros, esto no debería ser nada nuevo; el objetivo de cualquier suscriptor de seguros es evaluar adecuadamente el riesgo mediante la aplicación de la ciencia actuarial para asignar un valor monetario requerido para asegurarse adecuadamente contra ese riesgo.

Sin embargo, no deben cometer el error de creer que la gestión de riesgos solo es válida en lo que respecta a sus clientes. Las aseguradoras también deben protegerse a sí mismas.

Las aseguradoras recopilan una variedad de datos personales que los ciberdelincuentes pueden aprovechar para cometer fraude y otros delitos. Por lo tanto, la evaluación y gestión adecuadas de riesgos son extremadamente importantes para esta industria.

Se han enumerado cinco pasos para realizar una evaluación de riesgos eficaz.

Paso 1: Designar un administrador de riesgos

El administrador de riesgos puede ser un empleado, varios empleados o un proveedor responsable del programa general de seguridad de la información.

Paso 2: Identificar amenazas internas y externas razonablemente previsibles

Estas amenazas surgen de un posible acceso no autorizado, transmisión, divulgación, mal uso, alteración o destrucción de la información protegida. Además, las amenazas identificadas deben incorporar las de sistemas internos o proveedores de servicios de terceros.

Paso 3: Evaluar la probabilidad y estimar el daño

Teniendo en cuenta la naturaleza privada de la información que recopilan las compañías de seguros, deben evaluar la probabilidad de que los ciberdelincuentes apunten a las bases de datos de la compañía y estimen los posibles riesgos financieros, legales y de reputación.



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

Paso 4: Revisar constante de las Políticas. Procedimientos, Sistemas y Salvaguardias vigentes Determinar qué tan bien los controles en vigencia protegen los datos; esto proporciona información sobre las necesidades adicionales de ciberseguridad. Al revisar los sistemas de información, las compañías de seguros deben tener en cuenta todos los aspectos de sus controles. Para hacer esto, primero deben revisar y evaluar los diseños de redes y software.

También necesitan evaluar los riesgos que plantean sus procedimientos actuales de clasificación, gobernanza, procesamiento, almacenamiento, transmisión y eliminación de la información. Además, necesitan comprender qué también sus procesos actuales de detección, protección y respuesta protegen la información de ataques, intrusiones y fallas del sistema.

Por último, debe garantizarse una formación continua y relevante para empleados y directores.

Paso 5: Implementar procedimientos y salvaguardas

Una vez que identificadas las deficiencias en sus controles de ciberseguridad, implementar las medidas de mitigación necesarias para reducir el riesgo a cualquier tolerancia que haya definido su Directiva y/o Junta Directiva.

Más allá de eso, debe recordarse que: la efectividad de los controles de ciberseguridad cambiará a medida que las compañías de seguros incorporen nuevas tecnologías y a medida que los ciberdelincuentes desarrollen sus metodologías de amenazas. Por lo tanto, las compañías de seguros deben volver a realizar su evaluación de riesgos al menos una vez al año para asegurar la efectividad continua del control.

***¿En qué se diferencia la gestión de riesgos de la evaluación de riesgos?***

La evaluación de riesgos mide varios riesgos y ayuda a una compañía de seguros a definir los más importantes. La gestión de riesgos empresariales (ERM) para las compañías de seguros significa monitorear y actualizar los controles para los riesgos mitigados o aceptados, a menos que la compañía decida participar en una transferencia de riesgo, sin embargo, tal transferencia implica márgenes de riesgo para el asegurador, por ejemplo, en el hecho de asumir deducibles (como en cualquier seguro de Riesgo Financiero Puro).

***Pasos para la gestión de riesgos para profesionales de seguros***

Las firmas de seguros enfrentan regulaciones de seguridad cibernética a nivel estatal (**SIF**) y nacional, además de amplias expectativas de seguridad por parte de los bancos que trabajan con firmas de seguros. Agregando más complicaciones, la regulación de seguridad a nivel estatal será en su mayoría similar, pero no idéntica, en todas las jurisdicciones.

Cuando las compañías de seguros y los Ajustadores de Reclamos (internos o externos) administran adecuadamente el riesgo, les brinda una ventaja, no solo al ofrecer un control de pérdidas contra costosas filtraciones de datos, sino también al proteger a los corredores de seguros de violaciones de cumplimiento y mejorar su credibilidad con los clientes que buscan productos de seguros que puedan proteger a los las cosas más preciadas para ellos.



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

Lo más común sería establecer cinco pasos para la gestión de riesgos de las Compañías de Seguros (incluso de Intermediarios, Ajustadores y por supuesto Reaseguradores).

Paso 1: Diseñar un programa de seguridad de la información.

Un programa de seguridad de la información debe ser apropiado para el tamaño y la complejidad de cualquier profesional de seguros. Como parte del enfoque, una empresa puede optar por mitigar los riesgos por sí misma o transferir el riesgo a un proveedor. Sin embargo, si la empresa subcontrata servicios, debe asegurarse de que el socio de subcontratación también proteja la información confidencial.

Paso 2: Elegir los controles de seguridad adecuados.

Al igual que otros estándares prescriptivos, incluir una serie de controles que pueden ayudar a guiar al personal operacional, tanto de Colocación, como de Suscripción, Actuarial y de Reaseguro. Los 11 controles más recomendados y utilizados por los analistas de riesgos son:

1. Crear controles de autenticación y acceso.
2. Identificar datos críticos, personal, dispositivos y sistemas e instalaciones de tecnología de la información (TI).
3. Restringir el acceso físico a registros no solo de carácter sistematizado, sino incluso físico.
4. Incorporar cifrado en reposo y en tránsito.
5. Adopción de prácticas seguras de desarrollo de software.
6. Modificar los sistemas de información para mantener el cumplimiento del (de los) Programa(s) de seguridad.
7. Incorporar controles, como la autenticación multifactorial, para el acceso.
8. Probar y monitorear sistemas y procedimientos con regularidad.
9. Crear pistas de auditoría para detectar y responder a eventos de ciberseguridad que permitan la reconstrucción de transacciones financieras importantes, principalmente, por ejemplo, en pagos de siniestros, transferencias desde o hacia reaseguradores, y otros factores como el pago de instalamentos a Reaseguradores por adquisición de Contratos de Protección de Reaseguro Proporcional y No Proporcional entre otros.
10. Implementar medidas para proteger contra la destrucción, pérdida o daño por desastres naturales, incendios y daños por agua o fallas tecnológicas.
11. Crear procedimientos seguros de eliminación y retención de registros.

Paso 3: Ciberseguridad

Aunque existen métodos, procedimientos, guías, etc., parece prudente crear un enfoque de seguridad cibernética basado en **ERM** (**E**nterprise **R**isk **M**anagement), los modelos especifican que el proceso de gestión de riesgos empresariales debe incorporar la seguridad de la información.

Paso 4: Mantenerse informado.

Este procedimiento de gestión de riesgos se centra en compartir información sobre amenazas y vulnerabilidades emergentes. Como parte del monitoreo continuo, las compañías de seguros



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

deben estar al tanto de los nuevos vectores de amenazas. Como parte de la información a las partes interesadas internas y externas, deben establecer procedimientos de comunicación claros.

Paso 5: Capacitación en ciberseguridad.

Las normas modelo se centran tanto en la formación inicial como en la formación continua y actualizada para reflejar los nuevos riesgos para el ecosistema de datos y el medio ambiente. La repetición del procedimiento de "mantenerse informado" destaca la importancia de la conciencia cibernética de los empleados.

Con la cantidad de información personal recopilada por cualquiera de los actores participantes en actividades de seguros, la gestión de riesgos de seguridad cibernética debe ser una prioridad tan alta como la administración comercial diaria.

Dicho esto, las herramientas tradicionales como los calendarios compartidos para las asignaciones de tareas y los correos electrónicos para las discusiones toman el tiempo que podría emplearse mejor en monitorear la ciberseguridad. Mantener un programa de seguridad de la información eficaz requiere una herramienta de flujo de trabajo eficiente para coordinar la comunicación y la gestión de tareas entre las partes interesadas internas.

Lo anterior es válido para todo tipo de entidades vinculadas al sector asegurador, como servicios financieros, seguros de vida, seguros de salud o servicios de seguros de propiedad y accidentes.

Toda Entidad de vinculada al Mercado Asegurador o Reasegurador, debería disponer de un **Software de Cumplimiento de Normas de Protección** que le permite priorizar tareas. Todo el mundo sabe qué hacer y cuándo hacerlo, de modo que pueda mantener registros hasta el momento en que ya no sean requeridos o necesite deshacerse de ellos.

Finalmente, con adecuadas capacidades de seguimiento de auditoría, pueden documentarse las actividades de remediación para demostrar que se mantiene la confidencialidad, integridad y disponibilidad de los datos según las Normas previstas para el efecto, tanto de Control Interno como las exigidas legal o regulatoriamente.

**Evaluación de riesgos frente a análisis de riesgos**

Aunque pensamos que las palabras "evaluar" y "analizar" son intercambiables, no son lo mismo en el mundo de la gestión de riesgos.

Una evaluación de riesgos implica muchos pasos y constituye la columna vertebral de su plan general de gestión de riesgos. Un análisis de riesgo es uno de esos pasos, en el que se determinan las características definitorias de cada riesgo y se asigna a cada uno una puntuación en función de sus hallazgos.



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

**¿Qué es una evaluación de riesgos?**

Es común pensar que EVALUAR y ANALIZAR son indistintas e intercambiables, pero en realidad, en el ámbito de la Gestión de Riesgos no son iguales. Una evaluación de riesgos es un **estudio de todas las amenazas potenciales** para la capacidad de una organización para hacer negocios. Estos incluyen los riesgos del proyecto, los riesgos funcionales, los riesgos empresariales, los **riesgos inherentes** y los **riesgos de control**. Un **análisis de Riesgos** es uno de los pasos en el que se determinan las características definitorias de cada riesgo y se asigna a cada uno una puntuación en función de sus hallazgos.

> *El **riesgo inherente** y el **riesgo de control** son dos de las tres partes del modelo de riesgo de auditoría, que los auditores utilizan para determinar el riesgo general de una auditoría.*
> *El **riesgo inherente** es el riesgo de una representación errónea de importancia relativa en los estados financieros de una empresa sin tener en cuenta los controles internos.*
> *El **riesgo de control** es la posibilidad de una incorrección material en los estados financieros de una empresa porque no existen controles internos relevantes para mitigar un riesgo particular o los controles internos en funcionamiento no funcionan correctamente.*
>
> *Existe una clara diferencia entre el riesgo inherente y el riesgo de control. **El riesgo inherente** proviene de la naturaleza de la transacción u operación comercial sin la implementación de controles internos para mitigar el riesgo. **El riesgo de control** surge porque una organización no cuenta con controles internos adecuados para prevenir y detectar fraudes y errores.*
>
> *Toda transacción comercial tiene un riesgo alto, medio o bajo que las empresas deben mitigar mediante controles internos. Sin embargo, implementar un sistema de control interno no es suficiente.*
>
> ***Una organización también debe establecer revisiones periódicas para asegurar el éxito continuo del sistema para identificar y mitigar los riesgos de manera efectiva. Una organización tiene que revisar su sistema de control interno anualmente y actualizar los controles internos.***

*El tercer componente del modelo de riesgo de auditoría es el riesgo de detección, que es el riesgo de que los auditores no detecten una incorrección material en los estados financieros de una organización. El riesgo de auditoría es el riesgo de que los estados financieros de una empresa sean materialmente incorrectos, a pesar de que los auditores afirman que los estados financieros no contienen errores materiales.*

**Toda evaluación de riesgos debe constar de dos partes principales:** identificación de riesgos y análisis de riesgos. Cada uno de estos componentes, a su vez, comprende varias acciones importantes.



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

En seguridad, por ejemplo, las evaluaciones de riesgos identifican y analizan los eventos que representan las amenazas internas y externas para la integridad, la confidencialidad y la disponibilidad de los datos de la empresa.

El proceso de evaluación de riesgos de seguridad implica **identificar amenazas potenciales** a los sistemas, dispositivos, aplicaciones y redes de información; realizar un **análisis de riesgo para cada riesgo identificado** e **identificar controles de seguridad** para mitigar o evitar estas amenazas.

Los modelos de evaluación de riesgos de seguridad suelen incluir estos elementos:

- ✓ Identificar los activos tecnológicos críticos de la organización, así como los datos confidenciales que esos dispositivos crean, almacenan o transmiten.
- ✓ Creando un perfil de riesgo para cada activo.
- ✓ Evaluación de riesgos de ciberseguridad para todos los activos críticos.
- ✓ Mapeo de las interconexiones de todos los activos críticos.
- ✓ Priorizar qué activos abordar después de una violación de seguridad de TI.
- ✓ Desarrollar un plan de mitigación con controles de seguridad para cada riesgo.
- ✓ Prevenir o minimizar ataques y vulnerabilidades.
- ✓ Monitorear riesgos, amenazas y vulnerabilidades de manera continua.

Muchas organizaciones utilizan software de gestión de riesgos y cumplimiento para ayudarlas a gestionar todas las tareas asociadas con la evaluación de riesgos, el análisis de riesgos y la gestión de riesgos.

Los riesgos de seguridad no son el único tipo de riesgo que enfrentan las organizaciones. Aquí hay algunos otros:

- Riesgo financiero
- Riesgo de auditoria
- Riesgo crediticio
- Riesgo de cumplimiento
- Riesgo reputacional
- Riesgo competitivo
- Riesgo legal
- Riesgo económico
- Riesgo operacional
- Riesgo de terceros
- Riesgo de calidad



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

**Identificación: ¿Qué implica?**

Para la fase de identificación de riesgos, deberá usar su imaginación y visualizar los peores escenarios, desde desastres naturales hasta económicos.

¿Qué pasa si se produce un incendio en su edificio? ¿Qué pasa si alguien roba sus secretos de propiedad? ¿Y si la economía colapsara? ¿Qué pasa si el ransomware bloquea sus sistemas? ¿Qué pasa si un competidor rebaja sus precios? Etcétera.

Durante el proceso de identificación de riesgos, es importante tener en cuenta que no podemos ver el futuro. Podrían surgir nuevos riesgos para los que aún no tiene un plan. También es importante mantener abiertas sus opciones y que su proceso y programa de **gestión de riesgos** sea flexible. Planifique revisar su lista de riesgos con regularidad y establezca planes de contingencia para riesgos nuevos e imprevistos.

**¿Qué es un análisis de riesgo?**

En la fase de análisis de riesgos, examinará cada riesgo identificado y le asignará una puntuación utilizando uno de los dos tipos de sistema de puntuación: cuantitativo o cualitativo. Estos puntajes lo ayudan a priorizar sus riesgos y definir sus riesgos altos para que sepa cuáles debe trabajar para evitar o mitigar y cuáles puede ignorar o aceptar.

La puntuación cuantitativa asigna montos específicos a los factores de riesgo considerados.

a. ¿Cuál sería el costo para la organización si el riesgo se materializara? Esto se conoce como "expectativa de pérdida única" (**SLE**) **Simple Loss Expectation**

b. ¿Con qué frecuencia debe esperar que se materialice el riesgo? Una vez al año asigna una tasa anual de ocurrencia -**Annual Rate Ocurrence**- (**ARO**) de 1; una vez cada 10 años, un **ARO** de 0,1.

Para calcular el riesgo financiero en un año determinado, se multiplica **[SLE x ARO]**.

La puntuación cualitativa es menos específica y más subjetiva y utiliza una matriz de evaluación de riesgos. Una matriz que nos gusta involucra cuatro factores:

- **Probabilidad:** ¿Cuál es la probabilidad de que ocurra, que el riesgo se materialice?
- **Impacto:** ¿Qué tan duro se vería afectado su proyecto, función o empresa si ocurriera el evento?
- **Velocidad:** ¿Qué tan rápido sentiría el impacto su proyecto, función o empresa?
- **Materialización:** ¿Cuál es la gravedad potencial del impacto? Para llegar a este puntaje, sumar los puntajes de impacto y velocidad y dividir por 2.

Se pueden utilizar mitigaciones o controles para reducir las puntuaciones de un riesgo de impacto, velocidad y gravedad.

En el análisis de riesgos fase, también es importante para determinar el concepto de **riesgo apetito** y **tolerancia al riesgo.**



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

El marco de gestión de riesgos empresariales define el apetito por el riesgo como "la cantidad de riesgo, en un nivel amplio, que una organización está dispuesta a aceptar en la búsqueda del valor de las partes interesadas".

La tolerancia al riesgo, establece el marco, “refleja la variación aceptable en los resultados relacionados con medidas de desempeño específicas vinculadas a los objetivos que la entidad busca lograr”.

**Priorización de los riesgos**

Una vez que haya asignado puntajes a los riesgos, pueden clasificarse según su prioridad. Muchas empresas asignan clasificaciones de "**prioridad alta**", "**prioridad media**" o "**prioridad baja**". Definidos, por ejemplo, así:

**Alta prioridad**

Un ataque de **ransomware** (secuestro de datos), en el que los actores malintencionados usan malware para bloquearlo de sus sistemas y exigir un pago para restaurar su acceso, entraría en esta categoría. Lo mismo ocurriría con un ataque de día cero, en el que los piratas informáticos explotan una vulnerabilidad previamente desconocida.

**Prioridad media**

Un evento de riesgo medio podría ser un ex empleado que roba información después de haber sido despedido. La revisión de las políticas de acceso de los empleados de su organización sería un control contra la materialización de este riesgo, pero dado que la probabilidad de que ocurra es baja, lo más probable es que no necesite realizar esta revisión cada vez que alguien se vaya.

**Baja prioridad**

Si sus edificios están debidamente asegurados, la probabilidad de que alguien entre en sus oficinas y robe dispositivos podría ser baja. Si esos dispositivos no contienen ninguna información, la probabilidad de una pérdida de datos también puede ser baja o nula. Dado que no existe una urgencia asociada con este riesgo, se puede decidir revisar los controles de mitigación de riesgos de sus dispositivos anualmente.

**Automatización para obtención de los mejores resultados**

Haciendo un seguimiento de todo a la vez y todo el tiempo puede parecer imposible, especialmente cuando se trata de riesgo cibernético. Los actores de amenazas cambian y evolucionan continuamente sus tácticas y tecnologías, y la Compañía también debe hacerlo, o corre el riesgo de perder el control de sus sistemas, datos y marca.

La supervisión continua de los sistemas y redes puede informarle en tiempo real de las amenazas a la seguridad, pero debe tenerse cuidado: la solución puede enviarle un ping cada vez que haya una anomalía de cualquier tipo, generando falsas alarmas y provocando "fatiga de alertas" entre sus equipos.
Sin embargo, una buena solución de gobernanza, gestión de riesgos y cumplimiento puede ayudar a manejar las numerosas tareas asociadas con la gestión de riesgos de ciberseguridad.



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

Existen varios softwares que ayudan a identificar los riesgos al sondear los sistemas y encontrar brechas de ciberseguridad y cumplimiento. Ayuda a priorizar esos riesgos y asignar tareas a los miembros del equipo. Los paneles de control fáciles de usar permiten ver de un vistazo el estado de cada riesgo y lo que se debe hacer para abordarlo, y en qué orden.

También es posible generar una pista de auditoría de las actividades de gestión de riesgos y almacenar toda la documentación en un repositorio de "fuente única de verdad" para una fácil recuperación en el momento de una auditoría y permite auto-auditorías ilimitadas para que siempre se sepa dónde se encuentran los esfuerzos de cumplimiento y gestión de riesgos de la organización.

**El Riesgo Inherente frente al Riesgo de Control**
**¿Cuál es la diferencia?**

El riesgo inherente y el riesgo de control son dos de las tres partes del modelo de riesgo de auditoría, que los auditores utilizan para determinar el riesgo general de una auditoría.
El riesgo inherente es el riesgo de una representación errónea de importancia relativa en los estados financieros de una empresa sin tener en cuenta los controles internos.

El riesgo de control es la posibilidad de una incorrección material en los estados financieros de una empresa porque no existen controles internos relevantes para mitigar un riesgo particular o los controles internos en funcionamiento no funcionan correctamente.
Existe una clara diferencia entre el riesgo inherente y el riesgo de control. El riesgo inherente proviene de la naturaleza de la transacción u operación comercial sin la implementación de controles internos para mitigar el riesgo. El riesgo de control surge porque una organización no cuenta con controles internos adecuados para prevenir y detectar fraudes y errores.

Toda transacción comercial tiene un riesgo alto, medio o bajo que las empresas deben mitigar mediante controles internos. Sin embargo, implementar un sistema de control interno no es suficiente.
Una organización también debe establecer revisiones periódicas para asegurar el éxito continuo del sistema para identificar y mitigar los riesgos de manera efectiva. Una organización tiene que revisar su sistema de control interno anualmente y actualizar los controles internos.

El tercer componente del modelo de riesgo de auditoría es el riesgo de detección, que es el riesgo de que los auditores no detecten una incorrección material en los estados financieros de una organización.
El riesgo de auditoría es el riesgo de que los estados financieros de una empresa sean materialmente incorrectos, a pesar de que los auditores afirman que los estados financieros no contienen errores materiales.



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

**Los siguientes son ejemplos de opiniones de los auditores que son inapropiadas:**

- Proporcionar un informe de auditoría sin reservas, aunque la salvedad esté razonablemente justificada.
- Emitir una opinión de auditoría calificada, aunque la calificación no es necesaria
- No llamar la atención sobre un tema importante en el informe de auditoría.

El riesgo de auditoría generalmente se considera como el producto de los diversos riesgos que los auditores pueden encontrar cuando realizan auditorías. Es decir,

**Riesgo de Auditoría = Riesgo Inherente x Riesgo de Control x Riesgo de Detección**

El propósito de una auditoría es reducir el riesgo de auditoría a un nivel aceptable. Durante una auditoría, los auditores examinan los riesgos inherentes y de control relacionados con esa auditoría y, al mismo tiempo, obtienen una comprensión de la empresa y su entorno.

En consecuencia, los auditores deben realizar una evaluación de riesgo de cada componente del riesgo de auditoría y garantizar la exactitud de la información en los estados financieros. Dado que los inversionistas, acreedores y otros dependen de los estados financieros, el riesgo de auditoría puede conllevar responsabilidad legal para una firma de contadores públicos que realice las auditorías.

***Los tres elementos del riesgo de auditoría***

**Riesgo inherente**

El riesgo inherente se considera riesgo no tratado, es decir, el nivel natural de riesgo inherente a un proceso o actividad empresarial antes de que la empresa implemente cualquier proceso para reducir el riesgo. Esta es la cantidad de riesgo antes de que una empresa aplique controles internos.

Uno de los factores clave que genera el riesgo inherente es la forma en que una empresa realiza sus operaciones diarias. Una empresa que no puede hacer frente a un entorno empresarial que cambia rápidamente e indica que no puede adaptarse podría aumentar el nivel de riesgo inherente.

Otro problema que podría aumentar el nivel de riesgo inherente es la forma en que una empresa registra transacciones y actividades complejas. Se considera que una empresa que recopila datos de varias subsidiarias con la intención de combinar esa información más adelante está realizando un trabajo complejo, que podría contener errores materiales y dar lugar a un riesgo inherente.

Además, el riesgo inherente puede aumentar debido a la falta de integridad de la administración de una empresa. Por ejemplo, el liderazgo que participa en prácticas comerciales poco éticas podría afectar negativamente la reputación de la empresa, lo que provocaría una pérdida de negocios y aumentaría el nivel de riesgo inherente.



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

Otra situación que podría dar lugar a un riesgo inherente son las auditorías realizadas por auditores anteriores. Las auditorías que fueron débiles o sesgadas o las auditorías en las que los auditores ignoraron intencionalmente incorrecciones materiales podrían aumentar el nivel de riesgo inherente.

Las transacciones entre entidades relacionadas también podrían incrementar el nivel de riesgo inherente. Esto se debe a que existe la posibilidad de que el valor del activo involucrado en cualquier acuerdo financiero entre las partes relacionadas sea exagerado o subestimado. Una empresa puede mitigar el riesgo inherente mediante la implementación de controles internos.

**Riesgo de control**

El riesgo de control es la posibilidad de que los estados financieros contengan errores materiales debido a fallas en el sistema de controles internos de una empresa.

Si hay una falla importante de control, una organización probablemente sufrirá pérdidas de activos indocumentados, es decir, sus estados financieros pueden identificar una ganancia, aunque en realidad hay una pérdida.

El liderazgo de una organización es responsable de diseñar, implementar y mantener un sistema de controles internos que pueda prevenir adecuadamente la pérdida de activos. Sin embargo, no es fácil para una empresa mantener un sistema sólido de controles internos. Para mantener un sistema sólido de controles internos, la administración debe modificar el sistema periódicamente para adaptarse a los cambios en curso en el negocio.

Los riesgos de control ocurren debido a las limitaciones del sistema de control interno de una empresa. Si los sistemas de control interno no se revisan periódicamente, es probable que pierdan su eficacia con el tiempo. La gerencia debe revisar el sistema de control interno anualmente y actualizar los controles internos.

*Los siguientes elementos aumentan el riesgo de control:*

- No hay segregación de funciones.
- Los documentos se aprueban sin revisión de la dirección.
- Las transacciones no se verifican.
- El proceso de selección de proveedores no es transparente.

Las empresas deben decidir qué tipo de controles internos implementar para cada riesgo en función de la probabilidad de que ocurra el riesgo y el monto de la pérdida financiera si el riesgo ocurre.



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

La probabilidad y el impacto de un riesgo pueden ser altos, medios o bajos. Una empresa que cree que es muy probable que se produzca un determinado riesgo y que cause una pérdida financiera significativa debe implementar controles internos altamente efectivos.
Las empresas desarrollan controles internos para gestionar áreas que son inherentemente riesgosas una organización puede implementar controles internos para disminuir el riesgo de que las cuentas por pagar estén subestimadas.

*Ejemplos de dichos controles internos incluyen:*

- ✓ El director financiero revisa los detalles de las cuentas por pagar al final de cada período y determina si la lista está completa.
- ✓ El administrador de cuentas por pagar revisa todas las facturas que se ingresan en el sistema de cuentas por pagar.
- ✓ El administrador de cuentas por pagar pregunta a todos los empleados de cuentas por pagar sobre cualquier factura que no esté procesada al final del período.
- ✓ Los jefes de departamento revisan el informe de presupuesto a real.

El riesgo inherente existe independientemente de los controles internos. El riesgo de control existe cuando el diseño o la operación de un control no eliminan el riesgo de una incorrección material. Pero incluso después de que una empresa implemente los controles internos requeridos, no hay garantía de que el riesgo pueda eliminarse por completo. Como tal, parte del riesgo podría permanecer. Este tipo de riesgo se conoce como riesgo residual, ya que es el riesgo que permanece después de que la empresa implementa los controles internos.

**Riesgo de detección**

El riesgo de detección es el riesgo de que los procedimientos de los auditores no puedan detectar errores materiales en los estados financieros de una empresa.

Un auditor usa el modelo de riesgo de auditoría para comprender la relación entre el riesgo de detección y los otros riesgos de auditoría, es decir, el riesgo inherente, el riesgo de control y el riesgo de auditoría general, lo que le permite determinar un nivel aceptable de riesgo de detección.

Aunque el riesgo de detección no se puede eliminar por completo, el auditor puede manipularlo modificando ciertos factores, que incluyen:

- ✓ La composición del equipo del encargo, por ejemplo, la competencia y habilidad de los auditores y el tamaño del equipo del encargo.
- ✓ Los tipos de procedimientos de auditoría, por ejemplo, el grado de procedimientos sustantivos en comparación con las pruebas de controles internos, los procedimientos de recopilación de evidencia, incluso si la evidencia se genera interna o externamente.
- ✓ La rigurosidad de los procedimientos de auditoría, por ejemplo, el tamaño de la muestra y la duración del trabajo de auditoría.



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

- ✓ Control de calidad, por ejemplo, el sistema de control de calidad de la firma de contadores públicos certificados y revisiones por personal calificado fuera del equipo del trabajo de auditoría.

El riesgo inherente y el riesgo de control son conceptos importantes en la gestión de riesgos. Por naturaleza, las acciones comerciales están sujetas a diversos riesgos que pueden disminuir los efectos positivos que pueden traer a una empresa.

La diferencia clave entre el riesgo inherente y el riesgo de control es que el riesgo inherente es el riesgo sin tratar, es decir, el nivel natural de riesgo que es inherente a una actividad o proceso comercial sin implementar ningún control interno para reducir el riesgo. El riesgo de control, por otro lado, es la probabilidad de pérdida derivada del mal funcionamiento de los controles internos relevantes que una empresa implementa para mitigar los riesgos o la ausencia total de esos controles internos relevantes.

## LA LISTA DE VERIFICACION DE AUDITORIA DE GESTION DE RIESGOS EMPRESARIALES. UN MARCO INTEGRAL PARA DESARROLLAR EL PROGRAMA DE "ERM" Y ALGUNOS METODOS.

Las organizaciones empresariales se enfrentan a riesgos a diario. Deben determinar qué riesgos presentan una oportunidad para crecer y cuáles deben mitigarse. La gestión de riesgos empresariales (ERM) se centra en capacitar a estas organizaciones para que minimicen las pérdidas y maximicen la recompensa.

Pero desarrollar y ejecutar un programa de ERM puede ser una tarea ardua para una organización. Hay varios pasos complejos y evaluaciones que se deben realizar para garantizar que todas las bases de la empresa estén cubiertas y que la gestión de riesgos esté integrada en toda la organización.

Esta lista de verificación de auditoría de ERM proporcionará un esquema sólido para ayudarlo a e implica:

a. Realizar una evaluación de riesgos en profundidad para la organización
b. Analizar cada riesgo, su gravedad, tolerabilidad y prioridad.
c. Implementar capacitación en concientización sobre riesgos en toda la organización.
d. Determinar las medidas de mitigación de riesgos adecuadas para cada riesgo.
e. Integrar el monitoreo continuo del riesgo en su organización.

Las **listas de verificación** son herramientas que forman parte de los ciclos de mejora de la calidad del proceso asistencial, facilitan la comunicación entre los profesionales implicados, ayudan en la detección de fallos y **riesgos** e incrementan la seguridad del asegurado.



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

Las **listas de verificación** deben ser simples y fáciles de usar en terreno. El diseño debe ser simple, con elementos en un orden que sea lógico para la forma en que se inspeccionará cada tipo de actividad. Si es demasiado genérica, no será efectiva.

Algunos **métodos de análisis** de riesgos más utilizados y que más convengan a una organización de seguros son los denominados **FMEA (Failure Mode and Effective Analysis)** que contribuyen a determinar Frecuencia, Gravedad y Detección.

Los métodos de análisis de riesgos son técnicas que se emplean para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención para evitar peligros potenciales o reducir su impacto.

Es cierto que **no existe una única metodología de riesgos.** La forma ideal de realizar la gestión es seleccionar y combinar las mejores técnicas según el tipo de negocio o de proyecto. Por eso, a la hora de escoger, hay que tener en cuenta que algunas de estas herramientas son más idóneas para evaluar las causas de un problema, mientras que otras son más adecuadas para valorar las consecuencias.

Aquí presentamos algunos de los **métodos de análisis de riesgos** más utilizados para que elijas el que más le convenga a tu organización.

**What if**

El análisis *what if* (¿qué pasaría si…?) es una herramienta sencilla y fácil de entender para cualquier gestor. Usualmente se utiliza en la primera fase de la gestión cuando apenas se están identificando los riesgos. Después, este método puede complementarse con un análisis más profundo de los riesgos y sus causas a través de otras técnicas adicionales.

Esta **metodología de administración de riesgos** consiste en programar reuniones entre funcionarios o colaboradores que conozcan a fondo el proceso que se analiza. La primera reunión se programa para hacer lluvia de ideas, en esta se formulan preguntas que ayuden a visibilizar posibles problemas. De ahí el nombre de *what if*, pues cada una de esas cuestiones comienza de ese modo:

- ¿Qué pasaría si fallan los sistemas de cómputo y registro?
- ¿Qué pasaría si hay una interrupción de energía?

En las reuniones posteriores el grupo de expertos encontrará respuestas pertinentes para abordar todas las preguntas que se formularon, procurando hallar causas, consecuencias y recomendaciones. Justamente esa es una de las principales ventajas del análisis ***what if***, pues permite realizar una revisión exhaustiva de una amplia categoría de riesgos.



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal

***Análisis preliminar de riesgos (APR)***

Esta **metodología de gestión de riesgos** también forma parte del análisis inicial. Se utiliza para identificar posibles riesgos cuando el proyecto apenas está comenzando.

El primer paso en el análisis preliminar de riesgos es identificar todas las actividades que forman parte de un proyecto o de un proceso, intentando reconocer los posibles problemas que se puedan enfrentar en cada fase. Con esos datos se llena una tabla de registro. En una de las columnas se describen los riesgos que se identificaron, en otra se ubican las posibles causas, en la tercera se listan las consecuencias y en la última se sitúan las categorías de riesgos, combinando la frecuencia y la gravedad del riesgo para crear una clasificación de prioridades.

Cuanto más probable sea un riesgo y más graves sus consecuencias, mayor atención debe dársele. Con esos criterios, los riesgos se clasifican en menores, moderados, serios o catastróficos.

Para llevar a cabo esa priorización del riesgo, es conveniente utilizar una **Matriz de Riesgos**; y una manera simple de crear esta matriz, que permita visualizar los riesgos identificados, es a través de un software.

**Los 5 Por Qué´s**

El objetivo de esta técnica es llegar a la causa raíz de un problema específico, descartando las respuestas más inmediatas y superficiales. Así como los niños que empiezan a preguntar sobre el porqué de asuntos aleatorios, este método de análisis de riesgo es una indagación que consiste en formular preguntas iterativas sobre un problema determinado.

Esta **metodología de riesgos** debe desarrollarse en grupo. En primer lugar, se plantea el problema. Después, se pasa a la formulación de preguntas. Finalmente, a partir de las respuestas, se encuentra la causa raíz.

Contrario a lo que indica el nombre de la técnica, no es necesario que se restrinja el análisis a cinco preguntas. La cantidad de cuestiones estará determinada por la complejidad del problema que se pretende abordar.

**Juan Carlos Lancheros Rueda – CILA, BC´s Mech Eng, BC´s B.A, M.I.A, P.M.S, F.M.S.**
**C.E.O.**



NIT: 830.121.091 – 0
(601) 390 2846
www.valuative.co
info@valuative.co
Cra. 7 # 156 - 10 Of. 1607
Edificio Torre Krystal