Risk insight & compliance

QUANAM®

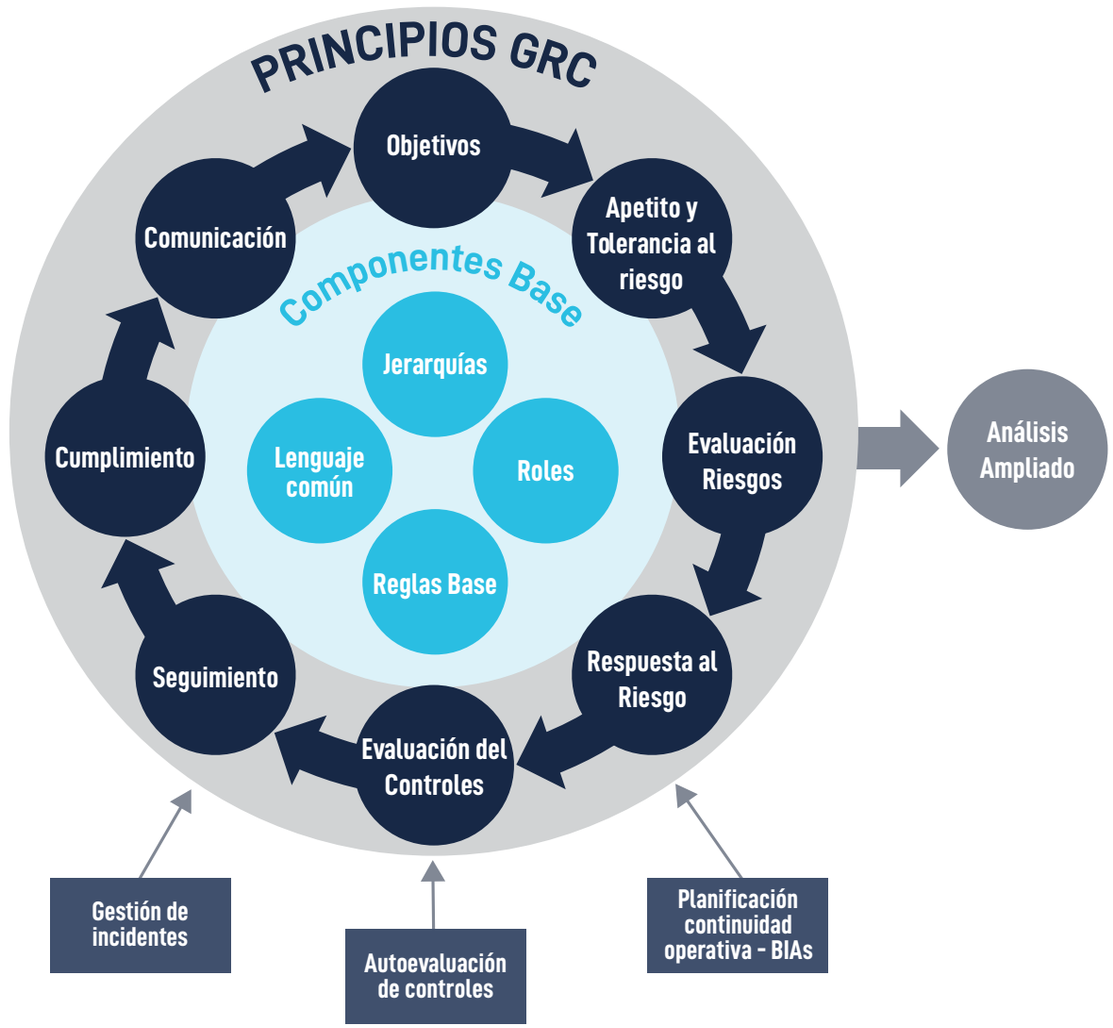
El desafío de una gestión de riesgo eficiente...

Risk Insight & Compliance es una plataforma que permite la implementación de una práctica robusta de Gestión de Riesgos, pudiendo aplicarse a:

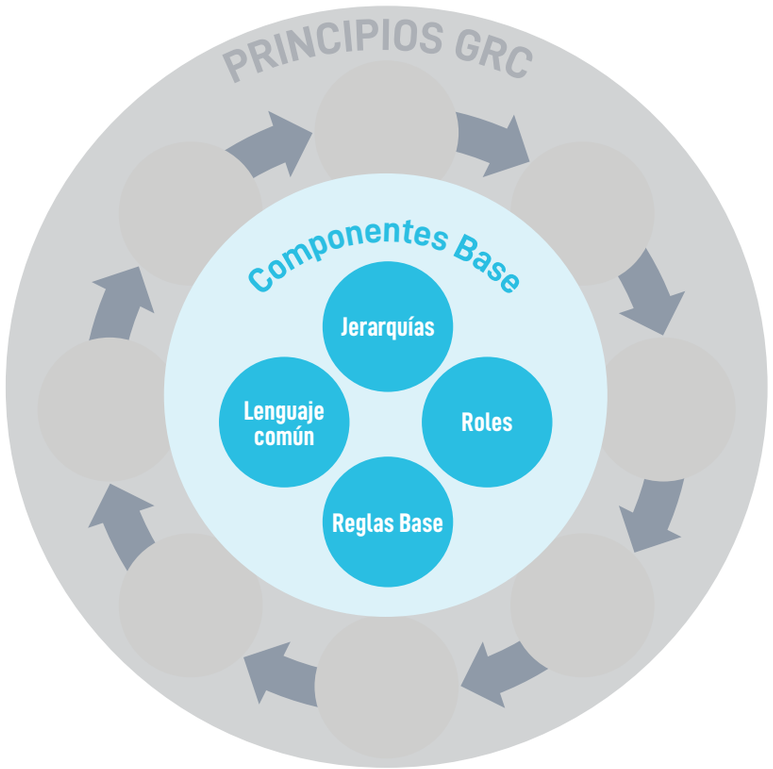
- procesos de gestión de riesgos operativos, de alcance corporativo (Enterprise Risk Management – ERM), aplicando los principales estándares internacionales correspondientes, como ser el Informe COSO II, la Norma ISO 31000:2018, etc.;
- procesos de gestión de riesgos de IT, alineados a lo requerido por la Norma ISO 27001, Cobit 5, etc.;
- procesos de gestión de riesgos de IT, alineados a lo requerido por la Norma ISO 27001, Cobit 5, etc.

RI&C asimismo, cuenta con funcionalidades adicionales que le permite soportar un molde de Gobernanza, Riesgo y Cumplimiento (GRC) bajo un eficiente enfoque convergente, que permite integrar estas prácticas en forma óptima.

RI&C puede ser utilizado por cualquier tipo de organización, independiente de su tamaño o Sector de actividad.



Componentes Base



RI&C promueve:

- La utilización de un **Lenguaje común** en toda la organización en relación a la Gestión de Riesgos, ya sean Operativos (ERM), Tecnológicos, de Proyectos o Portafolios; colaborando en la eliminación del abordaje por "silos" al trabajar en estas prácticas.
- Un claro entendimiento y asignación de **Roles y Responsabilidades** a través de distintos perfiles de usuarios, configurables; que permiten, por un lado, realizar un correcto control de acceso a la información, y por otro, que cada usuario consulte en forma sencilla sus tareas pendientes.
- El uso de diferentes **Jerarquías** para localizar riesgo, controles y evaluaciones, como por ejemplo la Estructura Organizativa de la organización, un Mapa de Procesos, Servicios, etc.; permitiendo consultar los mismos riesgos desde diferentes visiones.

Una característica importante de RI&C es que permite organizar todas las normas, políticas, leyes y procedimientos que la organización desea satisfacer, en forma estructurada, ordenada y centralizada, a partir de la definición de un conjunto de **Reglas Base.**

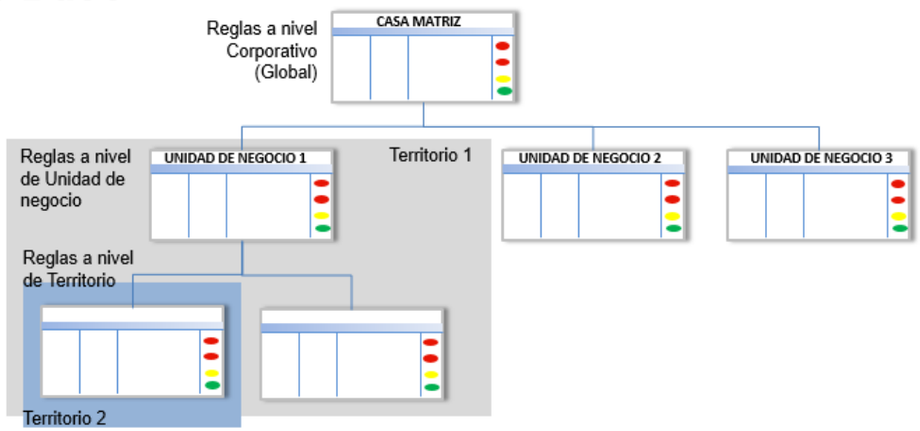
Las Reglas Base son flexibles y dinámicas; pudiéndose asociar a cada Jerarquía el conjunto de éstas que corresponde aplicar en cada nivel.

A partir de esta información RI&C permite verificar automática el nivel de cumplimiento que presenta la organización respecto al componente de las Reglas Base que se desee, mediante el análisis sistemático de los controles instalados.

De esta forma el Cumplimiento deja de ser una función en si mismo para pasar a ser el resultado de una Gestión de Riesgos bien realizada.

Existe una biblioteca de Reglas Base disponible, que recoge algunas normas y estándares internacionales que pueden resultar de interés como ser: Cobit, ISO 27000, etc.

Reglas Base



Principios de GRC

RI&C permite:

- Definir los **objetivos** que guiarán los análisis de riesgos. A medida que se van registrando objetivos, estos quedarán accesibles formando parte de un Universo de objetivos para su posterior utilización en caso que se desee.

El Dueño del proceso o componente sobre el que se realizará el Análisis de Riesgos es quien define los objetivos que guiarán la identificación de riesgos.

- Definir los diferentes **escenarios** con los que se llevarán adelante las evaluaciones de riesgos, a parir de la especificación de:
  - **heurísticos** a utilizar para estimar la probabilidad y el impacto asociado a cada riesgo; pudiendo aplicarse en el último caso criterios cuantitativos o cualitativos;
  - **fórmula para el cálculo de la Exposición** asociada a cada riesgo;
  - **Apetito y Tolerancia al Riesgo** que se desea aplicar para proceder a la clasificación de los riesgos.
- Realizar **Evaluaciones de Riesgos** aplicando diferentes escenarios; documentando el análisis inherente, el análisis residual así como las eventuales medidas de respuesta al riesgo que se deseen tomar: acciones de remediación (controles sugeridos), planes de contingencia y Indicadores Clave de Riesgos (KRIs); pudiendo asignar los responsables correspondientes en cada caso.

La medición de los KRIs puede realizarse en forma distribuida, generándose distintos tipos de reportes automáticos para llevar adelante su seguimiento.

Se puede definir un Flujo de Trabajo para guiar el desarrollo de las Evaluaciones de Riesgos desde que se encomienda su ejecución, hasta que es revisada, aprobada y cerrada.

También se puede prestablecer una frecuencia para actualizar o realizar determinadas Evaluaciones.

Todas las actividades e instancias son notificadas a los usuarios involucrados vía e-mail.

- **Consolidar** varias Evaluaciones de Riesgos de forma ponderada, generando información de apoyo a la toma de decisiones al nivel que se dese de la estructura Jerárquica que corresponda.

  En el caso de la Gestión de Riesgos Operativos y la Gestión de Riesgos de IT, esta ponderación suele realizarse a nivel de los objetivos utilizados como guía para identificar los potenciales riesgos; mientras que en Gestión de Riesgos de Portafolios de Proyectos se suele ponderar dependiendo de la relevancia de cada proyecto.

- Realizar la evaluación automática del nivel de **Cumplimiento** que presenta la organización respecto de cada uno de los componente incluidos en las Reglas Base (Normas, Políticas, leyes, etc.), a partir del análisis de los controles instalados incluidos en las evaluaciones.

- Una **Comunicación** fluida a partir de las consultas disponibles según el perfil del usuario y a través de los reportes predefinidos, de generación automática, tanto a nivel de una Evaluación en particular o del resultado de la consolidación de varias:
  - Mapa de Calor mostrando las Exposiciones Inherentes o Residuales
  - Detalle de una Evaluación, mostrando toda la información asociada
  - Listado de Controles Clave

- **Análisis Ampliado**

  RI&C cuenta con un módulo adicional que permite realizar la explotación de la información que administra utilizando herramientas de Analytics, con la flexibilidad que las mismas ofrecen.