

5. ISO 31000

Segons la norma ISO 31000, els principis per a la gestió de riscos són els següents:

- Crear i protegir el valor. Contribueix a la consecució d' objectius així com la millora de certs aspectes tals com la seguretat i salut laboral, compliment dels requisits legals, protecció ambiental, etc.
- Estar integrada en els processos d' una organització. No ha de ser entesa com una activitat aïllada sinó com a part de les activitats i processos principals d' una organització.
- Formar part de la presa de decisions. La gestió del risc ajuda a la presa de decisions avaluant la informació sobre les diferents alternatives

5. ISO 31000

- Tractar explícitament la incertesa. La gestió del risc tracta aquells aspectes de la presa de decisions que són incerts, la naturalesa d'aquesta incertesa i com es pot tractar.
- Ser sistemàtica, estructurada i adequada. Contribueix a l' eficiència i, conseqüentment, a l' obtenció de resultats fiables.
- Basar-se en la millor informació disponible. Els inputs del procés de gestió del risc estan basats en fonts d'informació com la pròpia experiència, l'observació i l'opinió d'experts.
- Estar feta a mida. La gestió del risc està alineada amb el context extern i intern de l' organització i amb el seu perfil de risc.
- Tenir en compte factors humans i culturals. Reconeix la capacitat i percepció dels empleats i persones interessades, això pot facilitar o dificultar la consecució dels objectius de l' organització.