

# La evaluación como herramienta en la Gestión de Riesgos

Generalmente, los riesgos se definen como los sucesos que pueden ocurrir en el futuro y que pueden tener un impacto negativo en la organización. Los riesgos pueden ser de diferentes tipos, como los riesgos financieros, los riesgos operativos, los riesgos legales, los riesgos tecnológicos, los riesgos de reputación, etc. En este artículo, vamos a hablar de los riesgos operativos, que son los riesgos que se relacionan con la actividad diaria de la organización. Los riesgos operativos pueden ser de diferentes tipos, como los riesgos de seguridad, los riesgos de calidad, los riesgos de cumplimiento, etc. En este artículo, vamos a hablar de los riesgos operativos de seguridad, que son los riesgos que se relacionan con la seguridad de la información y de los datos de la organización. Por ejemplo, un riesgo de seguridad podría ser la pérdida de datos debido a un ataque de ransomware. Este tipo de riesgo puede tener un impacto muy negativo en la organización, ya que puede afectar a la continuidad del negocio y a la reputación de la empresa. Por ello, es importante realizar una evaluación de los riesgos de seguridad de la información y de los datos de la organización. Esta evaluación debe tener en cuenta todos los aspectos de la seguridad de la información y de los datos de la organización, como la identificación de los activos de información y de los datos, la identificación de los riesgos de seguridad de la información y de los datos, la evaluación de la probabilidad de que ocurran los riesgos de seguridad de la información y de los datos, y la evaluación del impacto de los riesgos de seguridad de la información y de los datos. Por ello, también es importante realizar un cálculo del impacto, ya que no es lo mismo una multa por una inspección laboral que el robo de mercadería, ambos afectan a la organización, pero ¿cuánto me afectaría monetariamente estos dos eventos? Es la pregunta que se debe realizar para calcular el impacto.