

**Risk****Riesgos**

LÓPEZ, Fabricio†

*Universidad Iberoamericana*ID 1<sup>st</sup> Author: *Fabricio, López*

DOI: 10.35429/JEDT.2020.7.4.27.30

Received September 10, 2020; Accepted December 20, 2020

**Abstract**

A risk is the combination of the probability of an event and its consequence, according to the ISACA Cybersecurity Fundamentals Glossary . The risks can be financial, operational, technological, reputation, legal, continuity, etc. Risk management is a tool within the organizations that contribute to achieve the objectives established by senior management, allows efficient management of resources and, instead, helps to identify the risks to which the company is exposed. organization. Currently, Risk Management can be used in any field or environment of daily life, Information Technology is no exception. New information technologies such as the cloud, software as a service, security as a service, Internet of things, etc., open the range of possibilities in terms of risk. The development of new methodologies and considerations to evaluate the risks in Information Technologies, the use of a vision and creativity that allow the development of risk scenarios that have not been considered, explored or imagined in the past. This will allow organizations to be prepared for the occurrence of a threat and to be resilient, allowing them to continue with their operation.

**Trend, Risk, Future, Information Technologies****Resumen**

Un riesgo es la combinación de la probabilidad de un evento y su consecuencia, según el Glosario de Fundamentos de Ciberseguridad de ISACA. Los riesgos pueden ser financieros, operativos, tecnológicos, reputacionales, legales, de continuidad, etc. La gestión de riesgos es una herramienta dentro de las organizaciones que contribuye al logro de los objetivos establecidos por la alta dirección, permite una gestión eficiente de los recursos y, en cambio, ayuda a identificar los riesgos a los que está expuesta la empresa. organización. Actualmente, la Gestión de Riesgos se puede utilizar en cualquier campo o entorno de la vida diaria, la Tecnología de la Información no es una excepción. Las nuevas tecnologías de la información como la nube, el software como servicio, la seguridad como servicio, Internet de las cosas, etc., abren el abanico de posibilidades en términos de riesgo. El desarrollo de nuevas metodologías y consideraciones para evaluar los riesgos en Tecnologías de la Información, el uso de una visión y creatividad que permitan el desarrollo de escenarios de riesgo que no han sido considerados, explorados o imaginados en el pasado. Esto permitirá que las organizaciones estén preparadas para la ocurrencia de una amenaza y sean resilientes, permitiéndoles continuar con su operación.

**Tendencia, Riesgo, Futuro, Tecnologías de la Información**


---

**Citation:** LÓPEZ, Fabricio. Risk. Journal-Economic Development Technological Chance and Growth. 2020. 4-7: 27-30

---



---

† Researcher contributing first author.

## Introduction

The risks must be identified, evaluated and managed, supported by the risk analysis and from different approaches (Qualitative / Quantitative), an assessment of the threats is carried out to determine:

- The type of threat
- The causes of the threat
- The asset or assets affected by the threat
- The probability of occurrence of the threat
- The consequences of the threat

At this point the Probability of Occurrence (Very Low, Low, Medium, High, Very High) becomes a key element in Risk Management to be able to treat it.

The Risk Treatment seeks to find a balance between the level of security versus the cost of security, and the cost of protection versus the cost of exposure, with this information it will be possible to decide:

- Accept the risk
- Transfer the risk
- Reduce the risk to an acceptable level

There are multiple methodologies, norms and standards that allow analyzing and evaluating information security risks (OCTAVE, MAGERIT 2, ISO 27005, RISK IT ISACA, etc.).

The objective of this text is to document the presentation of Cybersecurity Trends 2018 exposed in the IT Security Topic class taught by Master Pedro Solares at the Universidad Iberoamericana, to students of Master in IT Governance.

- What are the current risk trends?
- What is the future of risk assessment methods in information technology?

## Context

### Current Risk Trends

Organizations such as the World Economic Forum (WEF) carry out studies to understand the risk trends that will define economic progress in the next years worldwide. In January 2017 the FEM presented the 12th edition of its Global Risk Report evaluating 30 global risks and 13 underlying trends that could aggravate or affect the interconnections between these risks<sup>1</sup>.

Within the report in the Top 5 of Global Risks in Terms of Probability, the following list is presented:

1. Extreme Weather Events
2. Involuntary Migration on a Large Scale
3. Major Natural Disasters
4. Large Scale Terrorist Attacks
5. Massive Incidents of Theft / Data Fraud



**Figure 1** Panorama of the Evolution of Risk 2007- 2017

The Massive Incidents of Theft / Data Fraud is in the category of Technological Risk and have interconnections with other global risks of different categories:

- Cyber-attacks - Technological Risk
- Rupture of critical information infrastructure - Technological Risk
- Adverse consequences of technological advances - Technological Risk
- Failure of financial mechanisms or institution - Economic Risk
- Terrorist attacks - Geopolitical risks
- Illicit Trade - Economic Risk

<sup>1</sup> The Global Risks Report 2017 12th Edition, World Economic Forum (2017), p.3, web page [http://www3.weforum.org/docs/GRR17\\_Report\\_web.pdf](http://www3.weforum.org/docs/GRR17_Report_web.pdf)



– Advanced Network Engineering

The assessment of security risks must adapt to emerging technologies and their nature of constant change, this will require the development of new skills even before changes are ready to emerge.

### Conclusions

– What are the current risk trends?

The trend is defined as a long-term pattern that is constantly evolving and that can influence to amplify the risks and / or modify the relationship between them. Changes in the landscape of international governments is an element of greater bias in risks, as well as climate change of the planet and that generates uncertainty in their behavior and effects, the cyber dependence that is observed in the increase in the interconnection of people, things and organizations, are the main trends that must be addressed and evaluated with the same speed as those presented.

– What is the future of risk assessment methods in information technologies?

The future is something that every minute changes and opting for a strategy that considers the constant evolution and changes in technology, as well as the risks that arise in its behavior, will help define the elements that allow an organization to be resilient to the threats to which it is exposed. CARTA is an approach that allows security professionals to adapt in real time and respond based on an operational context, improving the efficiency of the organization in terms of information technologies.

### Reference

Deloitte University Press (2017): Patterns of disruption - Anticipating disruptive strategies in a world of unicorns, black swans, and exponentials

Gartner (2017): Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats, <https://www.gartner.com/doc/3723818/use-carta-strategic-approach-embrace>

<http://expansion.mx/tecnologia/2017/07/25/los-duenos-de-tesla-y-facebook-pelean-por-la-inteligencia-artificial>

ISACA: Cybersecurity Fundamentals Glossary ISACA (2016), Risk, <https://www.isaca.org>

Secureworks (2017): State of Cybercrime Report 2017 <https://www.secureworks.com/resources/rp-2017-state-of-cybercrime>

World Economic Forum (2017): The Global Risks Report 2017 12th Edition <http://www3.weforum.org>