WHY IS IT IMPORTANT FOR YOUR COMPANY TO IMPLEMENT A SECURITY RISK MANAGEMENT PROGRAM AND HOW CAN YOU MAKE IT EFFECTIVE?

WHITEPAPER

Organizations are constantly exposed to a series of risks that can threaten them in various ways, whether financially, legally, or reputationally, among others. In the most serious cases, they can impede their continuity and even affect the physical integrity of their employees.

Ultimately, risk could be defined as the probability of an unwanted or unfavorable event occurring, in this case, for the organization.

Risk is composed of several factors, namely:

- **Probability: Risks can be very varied, but not all have the same probability of occurrence. While some have a high probability (for example, a cybercriminal sending fraudulent emails to employees), others are very unlikely (for example, a meteorite hitting a location where all information systems are located).**

- **Impact: On the other hand, it is necessary to know how the organization would be affected if the risk materialized. Are these consequences minor or would there actually be significant damage? As mentioned, these consequences can be of various types, such as financial, operational, strategic, reputational, or legal, among others.**

- **Uncertainty: Risk involves a degree of uncertainty, as it is not always possible to predict with certainty whether or when an adverse event or unfavorable situation will occur.**

- **Context: The perception of risk and its significance can vary depending on the context and perspective of individuals or organizations. What one person perceives as a risk may not be so for another, and what is considered a risk in one context may not be so in another.**

- **Tolerance: Closely related to the previous point is what is often called "risk appetite." While some people and organizations are very conservative and take few risks, others choose to expose themselves to a greater probability of suffering a negative event in anticipation of a greater reward if the unfavorable situation ultimately doesn't materialize. A very clear example is investments.**

In short, risk refers to the possibility of something negative happening in the future, and managing it involves taking steps to assess, mitigate, or control those possibilities and their impact to protect the interests and objectives of the organization and its employees.

To do this, it is necessary to know what risks they face. Depending on their type, risks can be classified as:

- **Financial risks: These refer to all the economic losses that can be suffered for various reasons.**
- **Operational risks: These are those that interfere with the proper functioning of the organization, such as those related to security or technological systems.**
- **Strategic risks: These relate to the organization's direction and positioning in the market.**
- **Compliance risks: This includes all risks related to compliance with current legislation, as well as the organization's own ethics.**
- **Environmental and social risks: These are related to the environmental and social impact of the organization's activities.**
- **Geopolitical risks: political events, international conflicts, and changes in the geopolitical environment that may affect the organization.**

It's important to emphasize that these risks are not mutually exclusive, and an organization can face multiple risks simultaneously. For this reason, it's necessary to have a risk management program that prepares for potential hazards. This document will analyze the basic concepts of a risk management program, the importance of having one in every organization, and how to implement it successfully, focusing on information security risks.

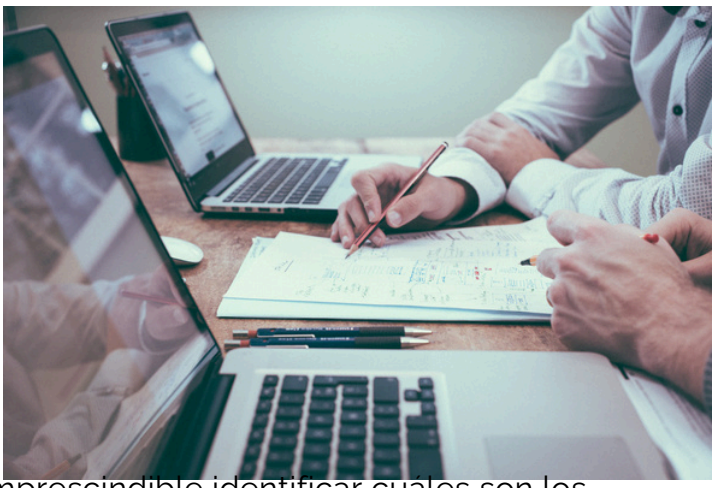
PROGRAMA DE GESTIÓN DE RIESGOS: CONCEPTOS BÁSICOS

Lo primero que se debe conocer si se quiere implementar uno de estos programas es, precisamente, qué es. Se trata de un conjunto de procesos, políticas, procedimientos y estrategias diseñados para identificar, evaluar, mitigar y controlar los riesgos que pueden afectar a una organización en el logro de sus objetivos. El objetivo principal de un programa de gestión del riesgo es ayudar a la organización a anticipar y abordar los riesgos de manera proactiva para minimizar pérdidas financieras, daños a la reputación y otros impactos negativos.

Como ha quedado patente, los riesgos pueden ser múltiples y de distinta índole, por lo que se deberán elaborar estrategias específicas para cada uno. Para acotar y evitar quedarnos en la superficie, en este documento nos centraremos en la seguridad de la información, tal como se ha mencionado anteriormente.

Los elementos de los que se componen los distintos programas de gestión del riesgo son los mismos, aunque pueden contar con algunas variaciones en función de las características específicas de los elementos a controlar:

- **Identificación de riesgos**



Es obvio que, para poder manejar una situación peliaguda de manera eficaz y eficiente, es necesario saber a qué nos enfrentamos. Como se ha mencionado, puede que, por la naturaleza de las diversas organizaciones, algunas de ellas se encuentren con riesgos específicos. Sin embargo, hay otros que son comunes a todas ellas, independientemente de su tamaño, sector o actividad.

En el caso de la seguridad de la información, es imprescindible identificar cuáles son los activos más importantes, y para ello se utiliza la clasificación en función de tres parámetros: la confidencialidad, la integridad y la disponibilidad.

La confidencialidad hace referencia a las personas que pueden acceder a dicha información. No todas las personas deberían estar autorizadas a ver ciertos documentos o consultar determinados datos.

Por otra parte, la integridad tiene que ver con la modificación o borrado de información no autorizados. Por ejemplo, nadie debería alterar los números de un reporte financiero una vez han sido revisados y aprobados. Por último, la disponibilidad indica la necesidad de que la información en cuestión se encuentre disponible para su acceso en el momento necesario. Mientras que hay información que debe estar permanentemente accesible, como pueden ser las páginas web de empresas de venta online, otros simplemente deben estarlo en momentos concretos.

RISK MANAGEMENT PROGRAM: BASIC CONCEPTS

The first thing you need to know if you want to implement one of these programs is precisely what it is. It is a set of processes, policies, procedures, and strategies designed to identify, assess, mitigate, and control the risks that may affect an organization in achieving its objectives. The main objective of a risk management program is to help the organization anticipate and proactively address risks to minimize financial losses, reputational damage, and other negative impacts.

As has been made clear, risks can be multiple and diverse, so specific strategies must be developed for each. To narrow the gap and avoid skimming the surface, in this document we will focus on information security, as mentioned above.

The elements that make up the different risk management programs are the same, although they may have some variations depending on the specific characteristics of the elements to be controlled:

- **Risk identification**

Obviously, in order to handle a difficult situation effectively and efficiently, it's necessary to know what we're dealing with. As mentioned, due to the nature of different organizations, some of them may differ. However, there are others that are common to all of them, regardless of their size, sector, or activity.
In the case of information security, it is essential to identify the most important assets, and to do so, classification is based on three parameters: confidentiality, integrity, and availability.
Confidentiality refers to who can access that information. Not everyone should be authorized to view certain documents or access certain data.
On the other hand, integrity relates to the unauthorized modification or deletion of information. For example, no one should alter the numbers in a financial report once they have been reviewed and approved. Finally, availability indicates the need for the information in question to be available for access at the necessary time. While some information must be permanently accessible, such as the websites of online sales companies, other information simply needs to be accessible at specific times.

- **Risk assessment:**

Once you know what you want to keep under control, you should consider the likelihood of it occurring and the severity of its consequences if it does. This will allow for prioritization in the subsequent management of each of these risks: thus, an event with a high probability of occurrence and a major impact will have higher priority than one with a low probability of occurrence and insignificant consequences. In the case of cyber risk, it is also worth considering what vulnerabilities may be found in the systems. Therefore, it is necessary to conduct frequent security tests and audits to verify that everything is in order and resolve identified problems to reduce the surface area exposed to an incident.

- **Risk mitigation:**

Mitigation is nothing more than reducing the likelihood of the negative event in question occurring and/or the impact it may have. To achieve this, different strategies must be followed depending on the type of risk we are facing. It is important to emphasize the term "reduction," since complete risk elimination is, in most cases, impossible, especially in the field of cyber risk. The human factor is a key element, since many security incidents that occur involve the organization's personnel in some way, whether voluntarily or involuntarily (as victims of a social engineering attack).

- **Communication:**

These measures taken must be appropriately communicated so that all employees are aware of them and can fulfill their role if necessary. Depending on the actions taken, this may also apply to third parties working with the organization.

- **Monitoring and control:**

When these strategies are implemented, they must be monitored to ensure they are being implemented properly and are having an impact.

- **Review and modification:**

If the measures taken prove to be suboptimal, they will need to be changed. It may also happen that certain strategies are effective at a given time but, over time, become outdated due to changes in the cyber, economic, political, social, and other landscapes.

INFORMATION SECURITY RISK MANAGEMENT: WHAT STRATEGIES SHOULD BE FOLLOWED?

Each organization has its own strategies depending on its characteristics. Without However, there are some points that are usually common to all programs.

- **Information Security Policy:**

The program's primary focus is the Information Security Policy. This is a comprehensive document that defines the general guidelines to be followed and the responsibilities.

- **Access control:**

As previously mentioned, not everyone should be able to access all information. Therefore, it's important to define who can view and/or edit different files and then restrict access to the necessary users. Furthermore, it's also important to keep information protected from third parties who might want to view or modify it for malicious purposes. Therefore, increasingly secure access methods are typically proposed as the sensitivity of the information increases (e.g., username and password plus a second authentication factor).

- **Monitoring:**

It's important to maintain control over the activity of users interacting with different information assets. To achieve this, various solutions are used, such as those that monitor files from their designated locations or that control intrusions by unauthorized individuals.

It's also important to have a change control system that allows for a record of when and by whom files that are categorized by the organization as confidential or simply important have been modified.

- **Information protection:**

Every organization handles sensitive data of any type, such as personal data or intellectual property. Therefore, it is essential to specify how it should be collected (in the case of personal data), stored, processed, and protected. This requires not only considering the organization's own criteria but also the legislation in force in each relevant territory.

- **Data Backup and Recovery:**

Information can be altered accidentally or by a malicious actor, as is the case with ransomware. Therefore, it is necessary to have backups and protocols for data recovery in the event of an incident. It is necessary to establish when and how these backups are made, as well as how to proceed if recovery is necessary. Furthermore, backups should be stored on an offline system if possible, or at least separate from the organization's main system. This should be done so that cybercriminals cannot easily hijack these backups as well.

- **Devices:**

Policies regarding devices used for work purposes can vary widely, but they should always exist. While some organizations only have one desktop computer, others also use laptops and mobile devices.
Others even allow the use of work (BYOD for “bring your own device”).

- **Incident Management:**

It's very likely that any organization will experience an information security incident at some point. These can be considered "major" or "small" depending on their impact, but it's important to keep in mind that even those that appear to have little consequence must be managed.

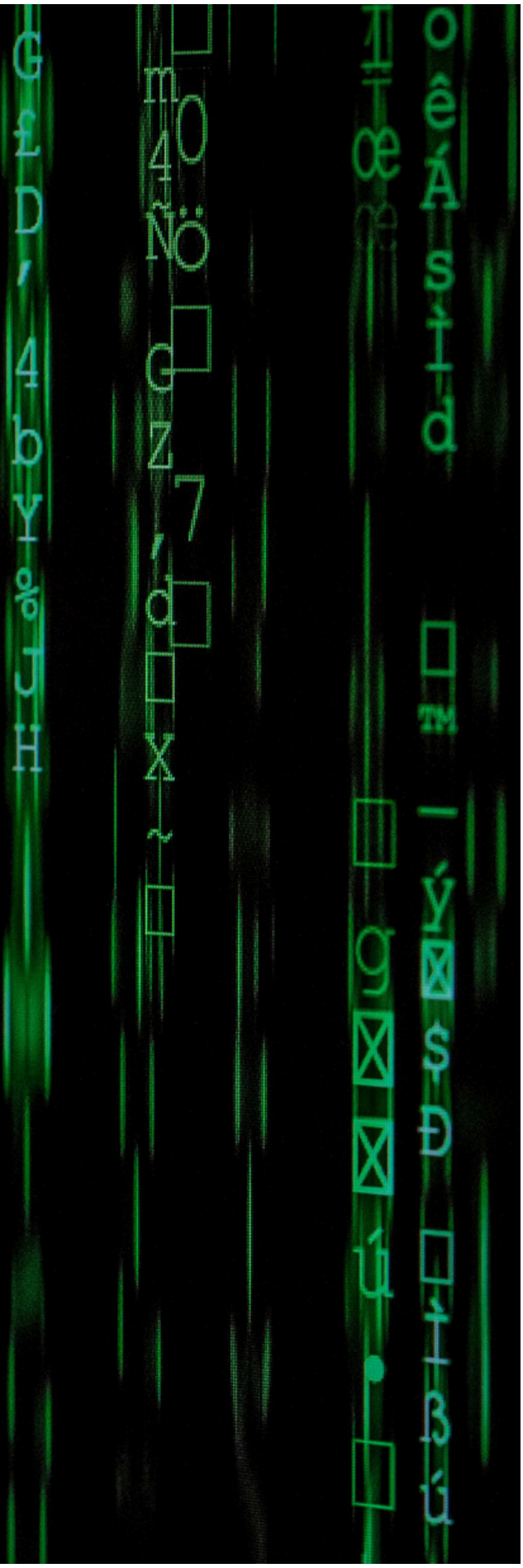
To achieve this, protocols must be established for employees to report any type of incident and for the appropriate team to respond to them if necessary. It is important to emphasize the importance of reporting anything that seems likely to be or become a security incident, even if suspicions are minimal. Employees often feel self-conscious when they are unsure, as they do not want to upset the Security team. For this reason, it is very important to create a climate of trust that encourages reporting any suspicions they may have, even at the risk of it being a false alarm.

- **Network Security:**

Devices aren't the only thing that needs to be protected: the organization's networks also need to be protected, including firewall configuration, intrusion detection, network segmentation, and traffic monitoring.

- **Email:**

Fraudulent or phishing emails are one of the main attack vectors used by criminals. Whether through general or personalized messages (spear phishing), cybercriminals seek to manipulate recipients into providing sensitive information or making bank transfers. Having a solution that identifies and filters these types of messages, or at least most of them, will help maintain information security, reducing the likelihood of employees falling victim to these scams. Furthermore, it is highly recommended that the solution include appropriate software that integrates with the email client used and allows users to report suspicious emails with the click of a button.



- **Awareness:**

Cybercriminals are increasingly focusing their attacks on the human factor. They use social engineering attacks to trick an organization into taking actions against it, such as providing sensitive information or making bank transfers. As mentioned earlier, their preferred method for this is usually phishing or spear phishing, but this isn't the only means they use. They also employ other methods, such as text messages (smishing), phone calls (vishing), or malicious QR codes.

Furthermore, as humans, we are very likely to make mistakes at some point that lead to a security incident, or to not know the guidelines to follow in this regard. For all these reasons, awareness is an essential element of a cyber risk management program.

- **Third-party management:**

Organizations often collaborate with others, whether suppliers, partners, or any other type of relationship. When joint activities are conducted or sensitive information is shared between the two organizations, it is necessary to define security requirements and sign confidentiality agreements to prevent the leakage of sensitive information.

These are just some of the main strategies to follow, but there are even more. The way you implement and carry them out depends on your needs. However, there are times when the final form of your information security risk management program is determined by other factors, usually with negative consequences. Below, we explain the main challenges involved in implementing one.

MAIN DIFFICULTIES:

- Inadequate organizational culture: Information security is an element that not all employees consider important. It's not unusual for them to believe it's an issue exclusively for the Security department or even the IT department. However, they aren't aware that it's a key aspect for the organization that requires everyone's collaboration. Therefore, it's important to emphasize the importance of the entire organization, at all levels, being involved in the process of strengthening it.

- Lack of commitment from senior management: Security culture begins at the top of the organization. Only in this way can measures be implemented to encourage all employees to take care of information security. However, it is not surprising that managers disengage from this task of maintaining information security, despite the fact that these are the profiles most targeted by cybercriminals. They often claim to have neither the time nor the money to allocate to this task, delegating everything to a security team that can do little without a budget, unaware that their example and involvement are key to the success of the strategy.

- Lack of resources: This is closely related to the previous point. The success of business operations is measured by their return on investment, or ROI, and has a tangible benefit; for example, the percentage increase in sales after introducing a new product is clearly observable after a specified period of time. However, this is not the case with information security, which is why ROI is used.

In these cases, the return on investment is not as evident, as it is not an increase in profits, but rather a decrease in losses. Therefore, in a society primarily focused on profits, it is not surprising that senior management considers investment in security to be at the bottom of the list of priorities, leaving a security team with a lot to do with an insufficient budget and, often, a limited number of hands.

- **Lack of awareness: One of the main challenges for the Security team is fostering the culture discussed in the first point. This requires involving all employees, but the most common challenge is an almost complete lack of security awareness. Therefore, it is necessary to establish specific plans to increase the alertness of the workforce. However, this point is something that, unfortunately, few address correctly. Simply offering a course once or twice a year doesn't work, and there is also no visibility into each employee's alertness or the human risk to which the organization is exposed, as well as its evolution over time. This management process often consumes a lot of the Security team's time, making the process inefficient and, despite efforts, often ineffective. In this whitepaper, we detail why current approaches don't work and how to change them to truly reduce the risk associated with the human factor.**

- **Resistance to change: This is very common among humans. We tend to settle into the procedures we're already accustomed to and to be somewhat reluctant to adopt new ways of doing things, rejecting change due to the uncertainty it can cause. However, in order to perfect the risk management system, it's always necessary to modify those parts that aren't working or that could be improved. Openness to change on the part of everyone in the organization is essential for implementing new solutions and procedures that can help increase its level of safety.**

- **Regulatory compliance: In addition to the importance of information security itself, current legislation must also be considered. Each territory has its own regulations, and organizations must follow them to avoid sanctions and any other consequences that may arise from non-compliance, such as legal consequences.**

- **New threats: Cybercrime is constantly evolving. New threats are developed or existing ones are refined every few years, making organizations increasingly vulnerable to them if nothing is done to counter them. Staying up to date with the latest developments and solutions is no easy task, but it is necessary to prevent incidents.**

- **Process complexity: The Security team's responsibilities are broad, and so will the number of tools used. Added to this large number is their complexity, which means they require a significant investment of time from those who manage them.**

These are just the main challenges typically associated with implementing an information security risk management program, but many more can arise. This makes their implementation very complicated, which is why these programs often fall short of the quality they should have.

So what does it take to successfully implement a quality program?

01

Involve senior management

The first step to ensuring a successful security risk management program is to involve senior management. This will require educating them on the importance of information security and allocating sufficient resources to a program that engages all employees. Communicating the benefits for the organization will be essential, supported by data such as the latest statistics, recent incidents from other organizations in the sector, or the estimated ROSI.

02

Create a culture of safety

It's important that all employees feel responsible for information security, as they all handle sensitive information to some degree or have minimal knowledge of how the organization works.

03

Allocate adequate resources

Of course, for a program to be sufficiently robust, it requires sufficient resources. Investment in security must be aligned with the organization's needs and encompass all aspects of a risk management program, leaving no stone unturned.

04

Have complete solutions that allow you to automate processes.

This point is closely related to the previous one. One of the most valuable resources for security teams is time, which is often consumed by various tools and tasks that, at the end of the day, end up requiring extensive manual attention. Therefore, finding solutions that encompass different needs will greatly simplify their work, especially if they are automated tools that require minimal interaction from this department without negatively impacting results.

05

Develop clear policies and procedures

A program may be of great theoretical quality, but it is of no use if the procedures to be followed are not sufficiently specific and explained.

06

Adapt the program to the needs of the organization.

Every organization is different, so procedures will need to be tailored to each one's needs and culture. For example, a company in the logistics sector doesn't have the same needs as one in the legal sector.

07

Comply with regulations

Each territory and sector has its own regulatory framework. It's important to pay attention to those that apply to our organization and act accordingly to comply with legal requirements.

08

Continuous monitoring and improvement

As stated above, a risk management plan is not static; it must be constantly evolving. Monitoring processes is necessary to evaluate their effectiveness and, based on these, improve them based on identified elements and the development of new threats.

09

Effective incident management.

Once an incident has occurred, it is necessary to respond to it to minimize its impact. This requires a solid plan that can be deployed quickly when necessary. Of course, every incident that occurs is an opportunity to improve both incident management and the overall prevention plan.

10

Putting people at the center

Often, the approach to risk management plans seems to leave people aside, forgetting that they are the ones who manage the information and the systems that contain it. Relegating them to the background and treating them as if they were just another machine or program on a list is a very common mistake that often ends up costing organizations millions of euros and/or destroying their reputation. Therefore, it is necessary to refocus the program so that employees, rather than a risk to be managed, become strong allies in maintaining security. For example, if a phishing message manages to overcome all technological barriers and finally reaches an employee's inbox, it will be essential to identify it and report it to the Security team.

HOW CAN KYMATIO HELP YOUR SECURITY RISK MANAGEMENT PLAN?

Kymatio® is a solution that prepares organizations and individuals against cybersecurity threats.

This SaaS solution for human cyber risk management uses neuropsychology and cybersecurity as the foundation of its technology. Kymatio®'s AI automates employee information security awareness programs, periodic employee alertness assessments, manages phishing attack simulations, and provides risk monitoring and mitigation services for exposed credentials.

Using neuropsychology and cybersecurity as the foundation of its technology, Kymatio® AI interacts with people, offering personalized awareness tailored to their needs, maintaining their alertness, and strengthening areas where they may be most vulnerable.

At the same time, it provides organizations with real-time visibility into human risk based on various metrics such as awareness level, roles and access to information, well-being level, response to simulations, and analysis of accounts exposed to breaches.

To learn more, contact us at contact@kymatio.com or schedule a meeting

ABOUT THE AUTHOR

Andrea Zamorano

Cyberpsychology Manager at Kymatio®, she researches the human side of cybersecurity and develops the algorithms necessary for the platform to accurately measure the factors involved, allowing it to assess risk and present personalized recommendations based on each individual's needs. She also teaches at the UAM School of Economic Intelligence (La_SEI) as an expert in indirect personality profiling. She is a psychologist by training, having studied at the Autonomous University of Madrid, and subsequently graduated from the Master's in Economic Intelligence and International Relations from La_SEI. She also holds a degree in Organization and Human Resources from the Autonomous University of Madrid.