In recent years, activism from human rights organizations and emerging media has become an activity full of increasingly large and complex risks. On the other hand, the very nature of this type of organization makes it difficult for practices to endure over time due to budgetary fluctuations, and equipment among others, making preparation and response to the growing threats seriously difficult.

This manual seeks to complement the work initiated by the community of facilitators in securing within civil society, making available to these and to the beneficiary organizations themselves a set of activities that allow generating organizational security policies in harmony with the real needs of each, adaptable to change and lasting over time.

Safe and Documented for Activism

SDA

sdamanual.org

SDA

Safe and Documented for Activism

sdamanual.org

Edited_ 2018
English edited_2018
Made in Chile

sdamanual.org
Author_Carlos Guerra Merlo
Design and layout_ Andrés Alaerkhon-S.
Translation to English_ Andrés Alaerkhon-S.
Collaborators _Mario Felaco
_Oriana Hernandez

Manual developed as part of the Open Web Fellowship from **Ford Foundation** and **Mozilla Foundation** within **Derechos Digitales Latin America organization**.

00_Intro

01_ License

When we mention this material's license we submit the license with which the repository is published, from where content used in this material is extracted, available in Github by the moment of publication.

MIT License

02_ Introduction

For many years now, organizations that defend human rights and emerging media have faced a myriad of threats and potential threats, whether from authoritarian states, business interests, extremist organizations or affected groups, among many others. Taking this into account, a need for security in operations of this type of organizations has only grown, increasing exponentially in the last decade when integration of different technological solutions available to operations of organizations becomes more widespread. Meanwhile, from the private industry and regulatory bodies, they began to develop specifications, frameworks and methodologies to generate security policies and protocols that would adequately protect data and resources of companies and enforce them with the law. However, the frameworks developed were extremely complex, long and expensive to implement for most civil society organizations that frequently manage tight budgets and inconstant funding cycles, which led to implementation of formal security policies that were exclusive and distant for most civil society organizations.

To attack this problem, many initiatives emerged that sought to increase the knowledge on information security towards civil society, organizations and activists, helping to generate criteria for tools selection and process design, implementing measures to safeguard information and other means. Some of these initiatives went further and generated methodologies to assess the organizations' security level, adapt content to specific groups or offer tools to the actual growing community of facilitators and coaches that serve organizations that most need to implement security in their operations. Although the appearance of these initiatives meant a crucial improvement for the security of the beneficiary organizations, there are still some spaces where the scope of the security strategies can be optimized, above all so that they last over time.

This manual endeavor to fill some of these gaps by adapting and simplifying methodologies available under private industry standards, mixing them along with other existing materials in the security area designed for civil society organizations and also with experience of several information security instructors in field with human rights defenders, organizations and independent media in Latin America for almost five years in a row at the time of publication of this manual. More specifically, this manual deliberately excludes certain processes and policies widely addressed in materials aimed at private industry in order to reduce to the essential the amount of activities and time that must be spent on its execution, understanding that the target organizations usually lack of time, resources or personnel to develop a security strategy as rigorous as proposed by standards such as NIST, COBIT or ISO among others. In the event that any organization wishes to deepen the development of security policies and strategies beyond this manual, in the references section, links or contents are made available in order to develop frameworks and methodologies to build documentation on security for organizations.

03_Who is this manual for?

This manual is a practical manual written to be used by information security facilitators who wish to complement their training and/or accompaniment work in civil society organizations (especially human rights defenders and independent media). However, it can be applied by people within this type of organization, external facilitators, not directly related to information security who are interested in the subject and practically any interested person that feels comfortable in following the instructions of these activities.

The content of this manual can also be adapted to any other type of organization that handles sensitive information, desires to increase security in the handling of it, and wishes to document security policies that last over time.

Objectives of this manual's application

- Establish security policies and protocols for civil society organizations adapted to their operations, and respond to the needs of their changing contexts and future projection.
- Increase the understanding of the security context within the members of civil society organizations at risk.
- Introduce civil society organizations (especially organizations defending human rights and independent media) in the threat model, risk analysis, and any other basic methodologies for surveying and assessing the level of organizational security.

04_ Methodology

How is the manual structured?

This manual is divided into 3 main sections, which contain a group of activities:

The first section seeks to explore the context of the organization and some of its internal processes, once the information is collected, the foundations of the organization's first security policies are established (Information classification policy and data retention policy).

The second section develops one by one other security policies through facilitated activities, while the third section introduces and guides the construction of concepts for threat models and security protocols, emphasizing the creation of risk matrices, succession plans, communications and protocol sequence.

At the end a section of references is exposed collecting links of projects, bibliographies and initiatives that complement the activities covered, as well as the next steps to extend, deepen and polish policies constructed from this material.

In each one of the sections we propose a set of activities that explain the facilitation process that must be followed to generate the proposed products, each activity has the following information:

- Estimated time of completion of the activity, which may vary depending on the size of the group, the skill of the facilitator and the steps considered in each activity to execute.
- Previous planning of the activity in terms of research or data collection of the organization.
- Materials required to execute the activity.
- Instructions of the activity, normally in a sequence of steps, listing actions to be carried out along with descriptive graphics if applied.
- Closure of the activity a summary of what has been achieved, and also what the generated products will serve to.
- References made during the development of the activity.

About references in printed version

The references are listed in the printed version and can be consulted from a web browser in two ways as shown below:

- sda.guerracarlos.com/referencias, navigate to the reference of interest and click.

01_ Research and security objectives

_ Definitions

- Stakeholder:
People, groups, formal or informal organizations that interact with us within a spectrum that ranges from allies to adversaries.

- Places where data is stored:
Physical and digital places where information is stored to be used, transmitted or archived. In the digital field, it coincides mostly with devices.

- Means of data transmission:
Channels used to transfer information between the work team or the organization and external allies. It applies to both traditional physical channels and digital media.

- Impact level:
The seriousness of the negative consequences that may occur after a specific event materialized.

01_ Objectives of the organization

Estimated time: 20 min

_Justification

This activity seeks to put the whole group on the same page regarding the reasons for being of the organization and the goals that it pursues. In the case of activist organizations, this can be a propitious moment to reinforce the concepts and values of social justice that motivate the group to do the work they do. In the case of media workers, the values of access to accurate information and freedom of expression which motivate journalists can be strengthened.

This section seeks the participants to put aside the stress produced by high workloads and concentrate on the internal motivations that lead each of them to be part of the team. It also works as an icebreaker to cope better with the development of the following activities.

_Input data

_Mission, vision and objectives of the organization.

_Products

_Direct

- Map of reasons why the organization exists from the point of view of the participants.

_Indirect

- Collective awareness, according to the objectives of the organization.
- Similarities and discrepancies between the perception of the team and the formal function of the organization.

_Previous planning

Find out if it is easy to obtain, mission, vision, objectives of the organization and prepare the corresponding material.

_Materials

- Post-its or sticky notes for participants.
- Papers printed or written with the mission, vision, and formal objectives of the organization or its equivalents in case they are presented in a different way.

_ Instructions

Depending on the number of participants and the convenience of the facilitator, the following steps are required, either individually or in pairs.

1.Distribute an adequate amount of post-its or sticky notes and markers among the participants.

2.Ask the participants to take 5 minutes to write on post-its or sticky notes the reasons why the organization exists, it can be helpful to raise sentences to complete as:

- The organization exists to...
- One reason for this organization to remain is...

3. After 5 minutes, ask the participants to stick the post-its or sticky notes on a specific place (wall, board or table), and then take a few extra minutes to group the notes that are very similar or just repeated. It is important that it seems easily evident when the same group has several associated notes, so it is not recommended to completely cover those similar ones.

4. Perform a summary based on what has been collected, putting special emphasis on common subjects found.

5.Show the mission, vision, and formal objectives available by briefly discussing the similarities and/or discrepancies that may exist between what has been collected back on the brainstorming, and what is actually formally written. If you find very marked differences, this could be a sign for:

- The organization to update its formal documents in order to reflect its evolution and current status.
- The organization to realize it deviated from its initial intentions, and should consider redirecting its actions to insert itself successfully in what was initially proposed.

In any case, this it is not the facilitator's responsibility to initiate an in-depth discussion about those differences, but to invite reflection and review at an appropriate time for the organization, maintaining a friendly and respectful language when recognizing the value the exercise had. For this methodology, knowing how the organization works **today** is enough to continue along with the activities, so these discrepancies should not affect the success in any work session.

_References

R1 A Step-by-Step Exercise for Creating a Mission Statement

02_ Stakeholder mapping and classification

Estimated time: 20 min

_Justification

In this activity, the main idea is to continue exploring the organization, gathering information directly related to its security, also necessary to raise an optimal threat model in the future. In addition, it is a valuable input to study the evolution of the organization, its environment, and changes in the corresponding threat model.

_Input data

- People, groups and institutions related to the organization.
- Core projects and processes of the organization.
- Information managed by the organization into its processes.
- Possible negative consequences when violating the information managed by the organization.

_Products

Direct

- Stakeholder map.

Indirect

- Group awareness about stakeholders of the organization.

_Previous planning

Research the organization well enough to have clear ideas of its stakeholders. This might help in case of starting or resuming brainstorming in the event that the group feels stuck or slow during the following activity.

_Materials

In case of doing the activity on paper:

- Post-its or sticky notes and markers or
- Large pieces of paper to stick on the wall and markers.

In case of doing the activity in digital equipment:

- Computer.
- Projector.
- Spreadsheet ready to fill, showing the headings with stakeholder categories.

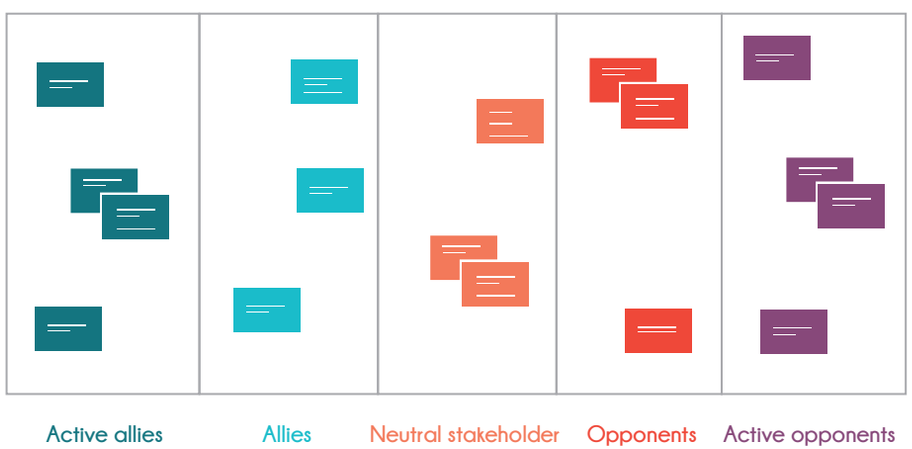
_ Instructions

Once the objectives of the organization have been related to the previous activity, it should be clearer for the participants about the approach of the group, the type of stakeholders linked to their work, and their motivations for the safety of the organization.

1. Explain briefly that the main idea is to create a spectrum of allies sorted by their attitude towards the organization, seeking to use just a few options in order to facilitate the process. Take for example the following:

- Active opponents
- Opponents
- Neutral stakeholder
- Allies
- Active allies

If the group and the facilitator, consider it necessary, they may spend a few minutes discussing the criteria by which the categories to be studied would be developed.



Graphic 1. Organization stakeholder mapping

2. Explain briefly that stakeholders are: people, groups and institutions, regardless of their formality as long as they have an existing or potential relationship along with the organization. For example, it is a good habit not to forget stakeholders like:

- Regulatory entities (taxes, work, communications).
- Utility companies.
- Providers.
- Maintenance personnel and general services.
- People to whom services are provided (victims, unprotected groups, citizens seeking advice, etc.).
- Similar organizations.

3. Ask the participants to say and / or write the stakeholders, so then afterwards being placed in the columns where they consider that they must located according to their judgment. If there is any disagreement with the rest of the audience in the chosen category, it can be discussed until there is consensus and the group is satisfied with all the names on the list.

4. Once the list is considered complete ask the participants for those stakeholders placed at the boundaries (active opponents and allies in the previous example). The main idea is to discuss not only the capabilities and motivations of these names in order to harm or help the organization, but also preparing participants for the data mapping and threat model activities.

5. Discuss along with the participants some considerations on stakeholder mapping:

- Maps of stakeholders may vary in time very quickly. Today an active ally tomorrow might be an active opponent, or a neutral stakeholder might take sides in the wake of a particular event.
- Categorization of the stakeholders is perceptual, perhaps for a group a certain name seems an ally, but in practice can play a different role unknown to the organization.
- Generally, an organization is linked to many more stakeholders than can be obtained in a 10-minute brainstorm. It is worthwhile for the group to feel comfortable applying this methodology so they can replicate it by themselves once they consider it convenient.

It is highly important that the map obtained to be available for future activities, if done on paper, it is recommended not to dismantle these post-its and / or sticky notes, but move them to a place where they are visible and do not interfere with other activities. In a case of doing the activity on digital equipment, it is recommended to have at hand the file where the information was collected.

_References

R2 Holistic Security: 2.3 Vision, Strategy and Actors Security First: ChampionsCurriculum

03_Data mapping and classification

Estimated time: 90 min

This activity is a variation of a dynamic proposed in several resources such as Holistic Security in its "2.4 Understanding and Cataloging our Information" section of Tactical Technology Collective or SaferJourno of Internews among others.

The idea behind this activity is to map all the data objects that the organization manages, to think about the possible consequences that commitment of these objects would have, to outline these possible consequences in a matrix of impact, and also associate the information objects managed with levels of impact on the matrix built.

_Justification

The main idea of this activity is to complete the information about the organization, and thus redirect it towards its sensitivity. In the process, the bases that will easily allow the construction of the first security policies for the organization will be established.

_Input data

- Stakeholder map..

_Products

Direct

- Matrix of possible consequences.
- Map of impact due to associated violations.

Indirect

- Group awareness about the sensitivity of the information handled.
- Criteria to classify information within the organization.

_Previous planning

In case of carrying out this activity on digital equipment, it is suggested to have a spreadsheet or other software with all the necessary fields and formats.

_Materials

In case of doing the activity on paper:

- Post-its or sticky notes and markers or
- Large pieces of paper to stick on the wall and markers.

In case of doing the activity in digital equipment:

- Computer.
- Projector.
- Spreadsheet ready to fill, showing the headings with stakeholder categories.

_Instructions

1. Brainstorm the pieces of information that the organization manages. It might include complaints from victims, leaked documents, research in process, accounting books, social media publications and/or public reports. No piece of legitimate information is of little relevance to this exercise.

- It is especially relevant to consider information on paper.
- Each idea should be written down on post-its or sticky notes or equivalent and be visible to everyone.
- You can move forward when there is consensus among the participants.
- More items can be added during the rest of the activity.

Graphic 2. Pieces of information mapping

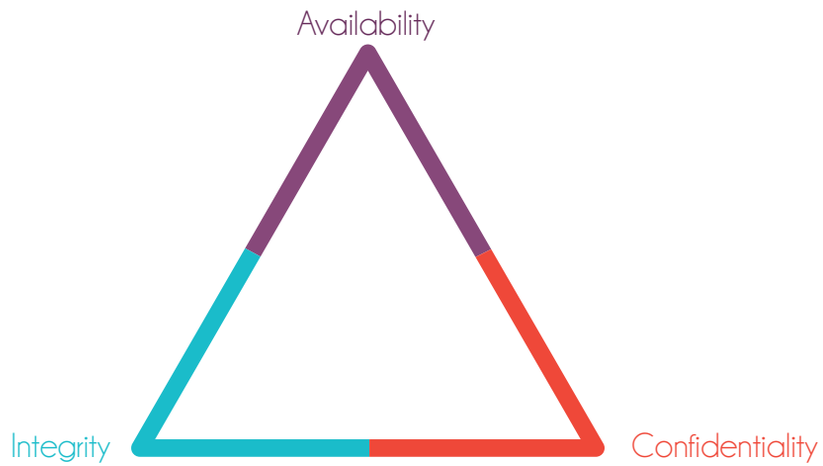
2. Along with the pieces of information into view, briefly explain the concepts of Availability, Integrity and Confidentiality, which are frequently used in information security to explain the different types of commitment to information. It is suggested to develop concise concepts and review other references to have a broader understanding:

Availability: It is the ability to always be within reach of those who need it. For example, when a server runs out of power, it threatens the availability of the information contained in it.

Integrity: Is the ability to be reliable, in the sense that its content has not been manipulated or altered by a third party. For example, for a malicious third party to take a database of victims and modify the information is considered a threat to the integrity.

Confidentiality: It is the ability to be accessible only to those who correspond by definition. For example, when a third party can read emails that are sent by two people, it is considered a threat to the confidentiality of the information transmitted by mail.

3. Discuss along with participants about the negative consequences the organization can meet in the event of compromising the information handled. Create apart from the brainstorming, a horizontal list based on types of consequences as shown in the figure 4.



Graphic 3. Triada CIA (Confidenfiality-Integrity-Availability).

▪ Digital consequences	▪ Physical consequences	▪ Emotional consequences	▪ Judicial consequences	▪ Administrative consequences	▪ Economic consequences

Graphic 4. Types of consequences

3. The point here is to generate a matrix in whose horizontal axis corresponds to this classification of consequences, a complete proposal (or simplified depending on the facilitator and the group) can be found below:

- Digital consequences: That affects the organization's online presence, e.g., related to social media, servers, mail accounts, services used by the internal team, etc.
- Physical consequences: Are those related to the integrity of people, objects and spaces, e.g., physical aggression, death, destruction of spaces, loss of resources, etc.
- Emotional consequences: Are those related to the psychosocial well-being of people involved with the organization, this not only includes the team, but also providers, beneficiaries, victims, etc. Frequently, some stakeholders are related to situations that create fears, stress, fatigue and traumas.
- Legal consequences: Those that affect the judicial integrity of people associated with the organization. Usually, they are related to arrests, withholdings, legal investigations, trials, etc.
- Administrative consequences: Are those related to the legal status of organizations and people beyond the judicial field. Frequently related to compliance with regulations, taxes, surveillance, loss of legal status, infractions of laws, etc.
- Economic consequences: Are those directly related to the loss of money and assets by the organization and/or its members.

These types of consequences are just hints. In case of requiring simplified this exercise, some of the proposed axes might be explicitly combined or excluded, even if the team considers it pertinent, new types may be added. For example, image or religious consequences (if applicable).

4.Once you have a clear understanding of all sorts of consequences, it is suggested to ask the participants to think about possible consequences of the commitment to pieces of information mapped in terms of availability, integrity and confidentiality, take note of these and place them on sticky notes or onto their digital equivalent below the type of consequence to which it belongs (digital, physical, legal, etc.)

- It is often expected that many consequences are repeated, in these cases with the Post-it or equivalent already existing will be enough.
- Thinking about availability, integrity and confidentiality is an aid to facilitate discussion and brainstorming of consequences, however, if the team feels comfortable on it, raising the possible consequences in other terms might work as well without any problem as long as they can be prioritized in the next step.
- It is expected the commitment to a piece of information may have consequences on more than one axis.

Some examples of consequences can be:

- Loss of legal status of the organization (administrative consequence).
- Death of complainants (physical consequence).
- Assaults on beneficiaries (physical consequence).
- Excessive fine (economic consequence).
- Waiver or dismissal of staff (administrative consequence).
- Loss of the website (digital consequence).
- Search warrant of the headquarters (judicial consequence).
- Drastic increase in levels of stress in team work (emotional consequence).
- Excessive increase in team workload (emotional consequence).

Digital consequences	Physical consequences	Emotional consequences	Judicial consequences	Administrative consequences	Economic consequences
The organization loses its website	Death of the beneficiary	Workload or to much stress	Detention	Loss of legal status	Loss of small amounts of money or equipment
The organization loses its Twitter account	physical aggressions to people	Traumatic event to people	Break in	Excessive fines	Bankruptcy of the organization
The organization loses its E-mails acconts	Destruction of office		Trial	Excessive administrative monitoring	Loss of large amounts of money or equipment
The office loses connection to the internet	Destruction of equipment		Prohibition of leaving the country		
Data from complainants leaked					
Accountable books leaked					

Graphic 5. Map of consequences.

5. After compiling a number consequences of each type, the idea of grading mapped consequences, according to their level of impact is introduced, then is later suggested to create a vertical axis that represents null, low, medium and high impacts. In the event that the facilitator and the team feel comfortable about it, you can change this scale to any other considered convenient (from 1 to 10, add to the proposed critical impact, etc.). After creating this axis, we proceed to locate the threats mapped into those different categories with the support of the team, as shown in the figure.Take this into consideration:

- It is possible to end up with some blank spaces, depending on the case it is worthwhile asking the team what consequences are missing in those spaces. In the case of low or null impact it is not mandatory to place direct consequences, this can be explained by the fact that everything that is considered below the consequence with the least impact is irrelevant.
- This part of the activity should own an adequate amount of time since it represents the pillar of the first security policy of the organization (data classification).

	Digital consequences	Physical consequences	Emocional consequences	Judicial consequences	Administratives consequences	Economic Consequences
HIGH	Data from complainants leaked	Death of the beneficiary	Traumatic event to people	Detention	Loss of legal status	Bankruptcy of the organization
	The organization loses its E-mails accounts	physical aggressions to people				
MEDIUM	The organization loses its Twitter account	Destruction of office	Workload or to much stress	Break in	Excessive fines	Loss of large amounts of money or equipment
	The organization loses its website			Trial		
				Prohibition of leaving the country		
LOW	The office loses connection to the internet	Destruction of equipment			Excessive administrative monitoring	Loss of small amounts of money or equipment
NULL	Accountable books leaked					

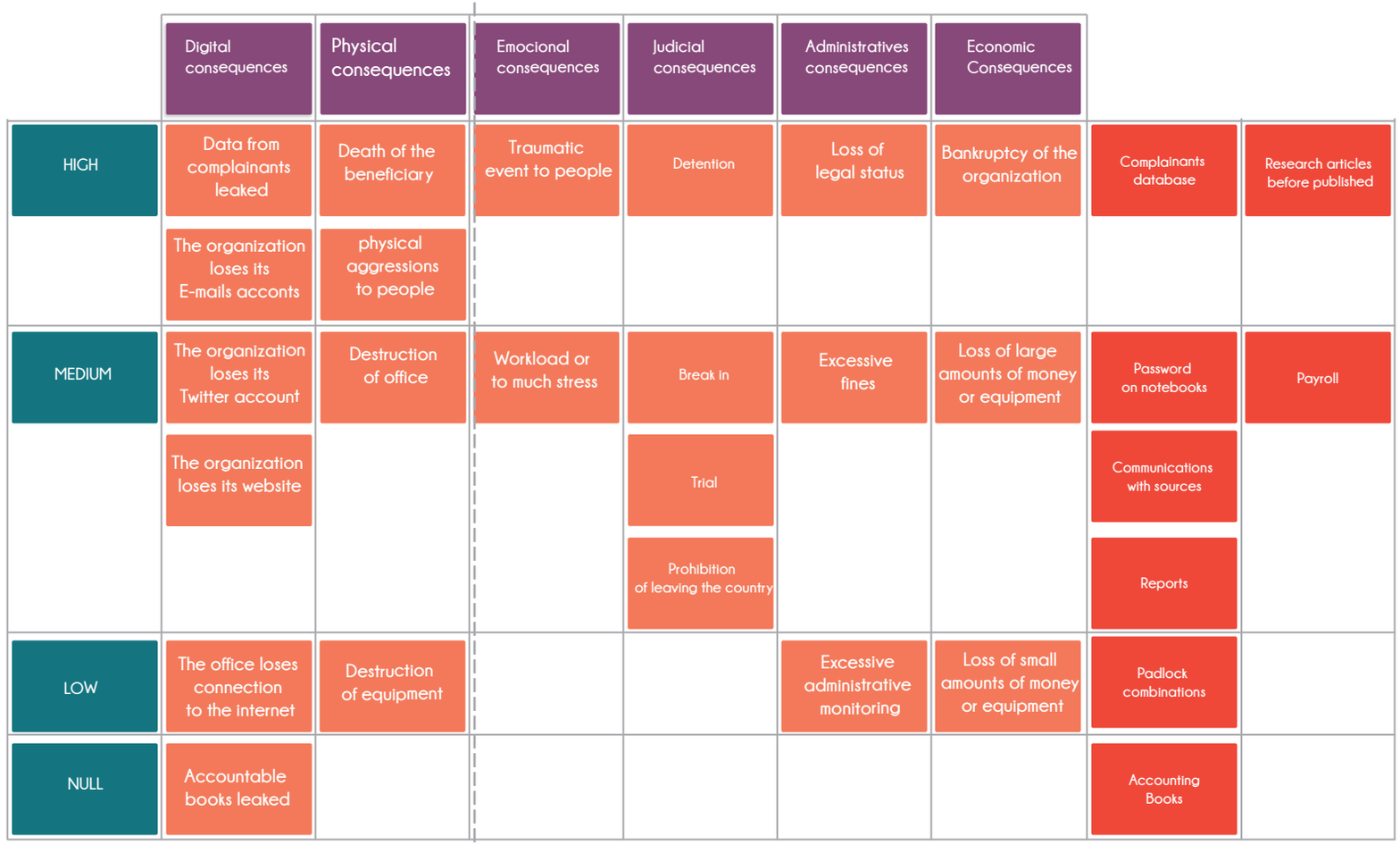
Graphic 6. Level of impact.

6.Once the team is satisfied with the consequence matrix, the pieces of data mapped at the beginning of the activity can be associated with the level of impact of the consequences corresponding to the commitment. This can be done in multiple ways, a proposal is available in the following graph.

_Closure of the activity

At the end of the activity you can discuss and emphasize what has been achieved:

- Axes of consequences were defined and associated with the data the organization manages.
- The bases of the data classification policy were established, so each time a new piece of information is handled, the level of impact associated with the commitment of this can be easily resolved, also along with the products that will be generated later, will be possible to determine safety measures to be taken.



Graphic 7. Data objects sorted by the level of impact.

_References

R3 Holistic Security: 2.4 Understanding and Cataloguing our Information
R4 SaferJourno
R5 Security First: ChampionsCurriculum
R6 Wikipedia: Seguridad de la información

04_ Information flow mapping

Estimated time: 90 min

_Justification

The main idea in this activity is to understand where the information lies, through which channels the information is transmitted, also to discuss the levels of security provided by these channels, and to associate data objects mapped in the previous activity in order to define key factors towards the construction of a data retention policy.

_Input data

- Matrix of possible consequences.
- Data map depicting impact due to associated violations.

_Products

Direct

- Data map listing places where the information lies.
- Data map listing channels through which information is transmitted.
- Basic security analysis according to where the information, lies and through which channel information is transmitted.
- Basic directives about handling of information according to their level of sensitivity.

Indirects

- Criteria for selecting secure transmission channels and storage places.
- Knowledge of which transmission channels and places should be used for existing and new data objects.

_Previous planning

In case of carrying out this activity on digital equipment, it is su- ggested to have a spreadsheet or other software with all the necessary fields and formats.

_Materials

In case of doing the activity on paper:

- Post-its or sticky notes and markers or
- Large pieces of paper to stick on the wall and markers.

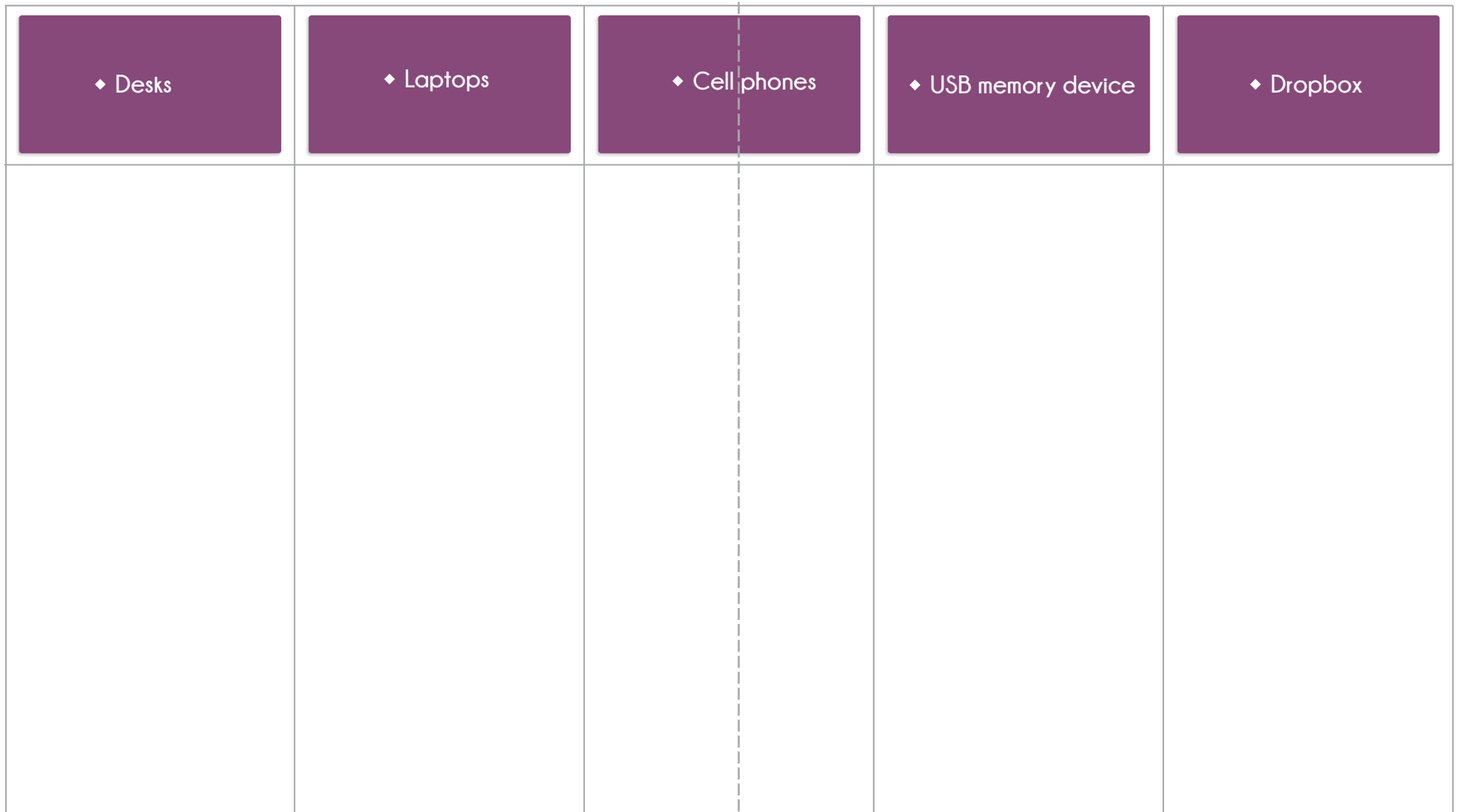
In case of doing the activity in digital equipment:

- Computer.
- Projector.
- Spreadsheet ready to fill, showing the headings with stakeholder categories.

_Instructions

1. Ask the participants to think and share places and devices where the data of the organization are stored. These can be on paper, digitally or in any other way. Now you can build column headers as shown in the figure: Some examples that may help the group to a better developed brainstorming are:

- Laptops and desktops.
- USB drives.
- Filing cabinets.
- External hard drives.
- Desks
- CDs.
- Internal server.
- Cloud storage services such as Dropbox or Google Drive.
- Mobile phones.
- Administrative and / or accounting software.



Graphic 8. Data storage places

2. Continue the brainstorming, but now ask the participants, through which means the information is transmitted. Add answers to the previous list as the chart shows:

Some examples that may help the group to experience a better developed brainstorming are:

- Conventional email.
- Messaging services such as WhatsApp, Signal or Telegram.
- Traditional mail service.
- Phone calls.
- SMS text messages.
- Encrypted email services such as Protonmail, Hushmail or Tutanota.
- Social networks.
- Web site.
- Remote management of equipment.

Graphic 9. Data transmission channels

3. Thinking about the headings of the columns written as one of the axes of a matrix, place on the vertical axis levels of impact used in the previous activity:

- It is important to use the same levels of impact if the participants defined differently to those proposed in this manual.

	◆ Desks	◆ Laptops	◆Cell phones	◆USB memory device	◆ Dropbox	◆ E-mails	◆ Cell phone calls	◆ SMS	◆ Whatsapp
HIGH									
MEDIUM									
LOW									
NULL									

Graphic 10. Data Matrix with Levels of impact.

4. Ask about the data objects in each level of impact where they are stored or transmitted. It is recommended not to take note of each data object, but to mark each coincidence of impact level associated with the storage location or means to transmit data. Ideally, it is recommended drawing the matrix on a large sheet of paper that allows to mark with X in the corresponding places as shown in the graph. 11.

- This step can be long, so you must take precautions when planning.
- It may help to have the post-its, sticky notes or equivalents of the previous activity for the data objects by impact level as a visual guide for the participants.

5. Introduce pertinent concepts about security for storage places and transmission channels according to the items held as storage places and means to transmit data.

- Encryption
- Point to point encryption.
- Insurance, locks, safes, etc.
- Accessibility of resources (Who has access to what).
- Considerations of services in the cloud.
- Etc.

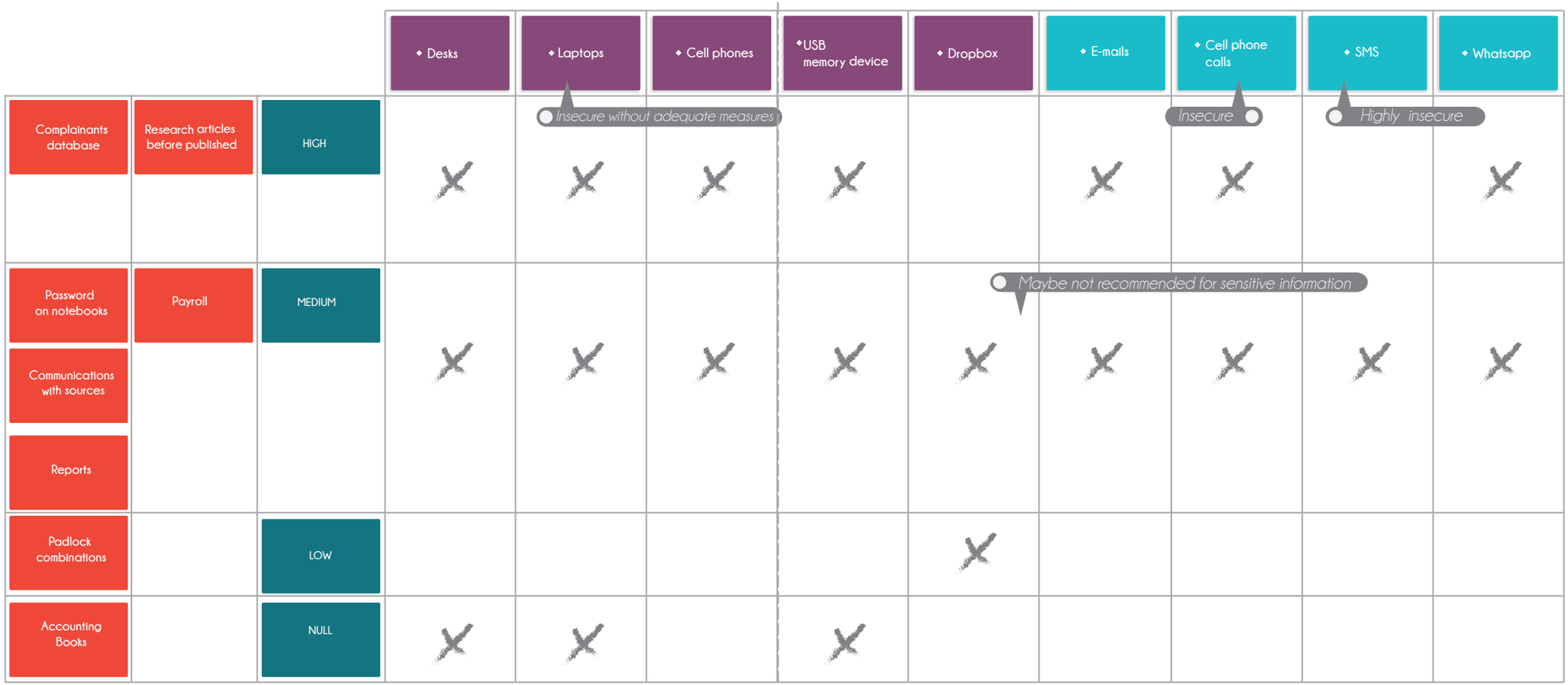
The success of this step is closely related to the knowledge that the facilitator as well as the group possesses about the equipment and services used. It may happen that in some activities there are services that the facilitator does not know about. It is important to ask the group not only what they know, but also to investigate any security considerations pertinent to unknown items.

			◆ Desks	◆ Laptops	◆Cell phones	◆ USB memory device	◆ Dropbox	◆ E-mails	◆ Cell phone calls	◆ SMS	◆ Whatsapp
Complainants database	Research articles before published	HIGH	X	X	X	X		X	X		X
Password on notebooks Communications with sources Reports	Payroll	MEDIUM	X	X	X	X	X	X	X	X	X
Padlock combinations		LOW					X				
Accounting Books		NULL	X	X		X					

Graphic 11. Means of storage and transmission of data by level of impact currently employed in the organization.

6. Discuss along with the group if there are considered unsecure channels in which sensitive information is stored or transmitted. Some key questions can be:

- Are some of the above considered unsecure channels?.
- Are some of these storage places easy to access for unauthorized people?.



Graphic 12. Data map analysis

7. Suggest to the group a modification in the matrix where it is defined what type of information per level of impact should be in each column, and the pertinent considerations in each case (if a computer must be encrypted to contain certain information, if you must use VPN or https to access a specific resource, etc.).

- The use of another color can be effective and useful to work on the same matrix, makes the activity easier to see the differences between what is currently done in the organization and what should be done from that moment on.

			◆ Desks	◆ Laptop	◆ Cell phone	◆USB memory device	◆ Dropbox	◆ E-mails	◆ Cell phone calls	◆ SMS	◆ Whatsapp
Complainants database	Research articles before published	HIGH		Device or file encryption				PGP encryption			SIGNAL
Password on notebooks Communications with sources Reports	Payroll	MEDIUM	Clean desk policy	Device encryption	Device encryption and password			2 factor authentication Gmail			
Padlock combinations		LOW									
Accounting Books		NULL								Emergency cases	

Graphic 13. Means of storage and transmission of data by level of impact for the organization

_Closure of the activity

At the end of the activity you may discuss and emphasize all what has been achieved:

- Several forms of communication and places for data storage were mapped.
- The data objects of the organization were associated with channels and storage places.
- Discussion began based on the level of security of the means used to store and transmit data, and establish basic premises from which the data retention policy of the organization will be built on.

It is necessary to take into account that in order to elaborate a complete data retention policy it is important to consider other things besides the means of storage and communication of the data objects, for example:

- For how long each data object should be in storage (expiration of data).
- How data objects should be deleted by expiration.
    - E.g.,: Prepare annual reports of complaints that will be deleted.

- Who manages the data: implementation of the principle of minimum privilege.
- Who are the decision-makers in terms of creation, storage and custody of the data.

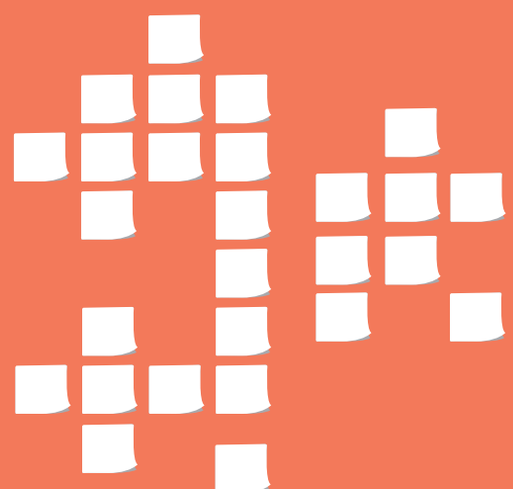
_References

R7 What is encryption? - Surveillance Self Defense | EFF

R8 Protect sensitive files in your computer - File encryption | Security in a box

R9 Communicating with others - end-to-end encryption - Surveillance Self Defense | EFF

R10 Secure Messaging Scorecard | EFF - Although it is outdated it is still a valuable resource to consult.



02_ Policies and Directives

_ Definitions

- Security policy:
  A formal document that collects the security strategies that an organization takes in specific areas of its operations, provides an overview of the organization's security status, the objectives it pursues in terms of security and criteria to determine possible exceptions to the policy or actions to take in situations that escape the current scope of the document.

- Security Directive:
  Set of specific rules that are implemented by the work team and its relevant allies to implement security policies in daily work. These directives can be more specific in the use of specific tools and equipment and can change over time more frequently.

01_ Introduction to security policies and directives

Estimated time: 15 min

_Justification

Before starting activities that seek to generate documents containing security policies and directives, it is very important that the participants understand what they are and what they are for, reducing errors, improving the flow of activities and involving the participants better. The idea behind this is to introduce the concepts of security policies and directives.

Unlike other activities in this manual, the present is more of an expository nature and less interactive. To the extent that the facilitator feels comfortable, it is recommended to design an activity that manages to introduce the concepts.

_Products

_Indirect

- Team knowledge of the concepts of security policies and directives..

_Previous planning

In the event of requiring some audio-visual material such as presentations, videos or papers with the concepts addressed and/or examples.

_Instructions

1. Expose the concept of security policy to the group:

> Security policy: It is a formal document that collects the security strategies that an organization takes in specific areas of its operations, providing an overview of the organization's security status, the objectives it pursues in terms of security and criteria to determine possible exceptions to the policy or actions to be taken in situations beyond the current scope of the document.

This concept can be proposed as the union of several ideas:

- It is a written document.
- Describes security objectives and strategies.
- It must cover as many cases as possible in the areas that define it.

In addition to these considerations, the security policies should be aligned with the mission and vision of the organization, in order to be designed so that they can be applied for long periods of time without requiring any major changes. It is normal for policy reviews to be made only when some of these conditions are met:

- A long period of time has passed since your last review. Normally in the order of the years (e.g., between every 3 and 5 years).
- There was a security incident which clearly showed that the policy is not effective in a certain scenario and must be reformulated to better face future risks.
- There was a significant change in the mission and vision of the organization and the policy should be refreshed to adapt to the change in operations.

Security policies must be respected by all members of the organization, for this reason, it is important that those in charge of management and operations are involved in the process, approve these policies and help their compliance during daily basis operations.

2. Expose the concept of the security directive to the group:

> Security Directive: Set of specific rules carried out by the work team and its relevant allies to implement security policies in daily work. These directives can be more specific in the use of specific tools and equipment and can change over time more frequently.

This concept can be proposed as the union of several ideas:

- They are specific rules.
- Its mission is to help compliance with the policies.
- They relate to the day-to-day processes.

Since security directives are quite more dependent on common technologies and practices, they are designed to be revised and changed much more frequently than policies, as a general guide it is suggested to review the directives when any of these conditions are met:

- An amount of time has passed and now some security practices could be questioned or improved thanks to discoveries or updates. Take for example, when a critical vulnerability is discovered in a tool or when a new product emerges improving the conditions of the organization's processes so is desirable to be implemented. Normally these times are measured in months (e.g., between every 3 to 12 months).
- There were changes related to security policies, including ones as a result of security incidents that affect the policy in question.

In general, the security policies own a clear instructional language, specifying specific actions to take in certain scenarios, take for example:

- X piece of information is transmitted through these channels: ...
- It is not allowed to use the Y device to store highly sensitive information.
- Z piece of information can be transmitted by the W channel under the following conditions: ...

Remarkable differences between security policies and directives are:

- Its scope: the policies are general and the directives are specific.
- Its dependence: security policies are a part of security policies.
- Its evolution over time: generally security policies change in the order of the years, the security directives in the order of the months.

In many of the information security reference frameworks, the concept of security policy is represented under other documents or names and may generate confusion when consulting other types of literature. In this case, the most important thing to adapt this concept is to understand that it is about clear instructions to execute a determined action complying with the security policies, in this manual the concept of a directive is abstracted to build a model that is fast understanding and facilitation for the target groups.

_Closure of the activity

In this training activity the concepts of security policy and directive were explored in a rigorous manner, which will allow us to progress effectively in the following activities.

_References

R11 Information Security Policy Templates | SANS Institute

R12 Introduction to Security Policies, Part One: An Overview of Policies | Symantec

R13 Information Security Handbook: A Guide for Managers | NIST

02_ Data protection policy

Estimated time: 60 min

_Justification

One of the core aspects of any organization is the manipulation of data given that any carried out process can be abstracted to the generation, processing, storage, and publication of information. In the case of organizations performing activism or documentation in the area of Human Rights, there is an important variety of types of information whose commitment may trigger negative consequences for any organization, its members or related actors. The idea of developing a data protection policy is to establish a series of guidelines that help to treat each piece of information in the most appropriate way possible according to its sensitivity.

_Input data

- Data mapping developed in the section Data mapping and classification.
- Information flow mapping developed in the section Information flow mapping.
- Template 1: Data protection policy open in a team to fill it up during the course of the activity.

_Associated Concepts

- Sensitivity data levels: It is a scale by which is established how much a piece of information is considered delicate and needs to be protected.
- Principle of the minimum privilege: Proposes that data should be accessible only to those people who need to use it within their usual processes.
- Responsible for the information: Are those people with direct competencies in the manipulation of information.
- Disposing of information: Refers to the techniques used to dispose of data pieces once they have reached their useful life or that must be destroyed for any kind of regulations and safety reasons.

_Policies to be developed

Data Protection Policy to be developed in this activity, abstracts existing content in the following policies described in standardized reference frames:

- Data classification policy: Defines criteria by which the sensitivity level of the information handled is determined, and strategic lines of management of this information at the proposed sensitivity levels. It also usually delineates those responsible for managing and safeguarding this piece of information worked on in the organization.
- Data retention policy: Defines, among other things, the time the organization can keep certain types of sensitive information, how to dispose of it, when it is removed, in which devices, which security practices should be applied to each type of sensitive information, and how sensitive information is processed according to legal regulations and best practices.
- Data access policy: Defines the pieces of information that can be accessed and manipulated by the different groups of the organization, in order to diminish the possibilities of commitment of the same and to make more efficient the information flow within the processes of the organization.

_Guiding questions

1. What is the scope of the proposed policy?
2. What levels of sensitivity does the information handled by the organization have and how are they
3. described?
   - How can any piece of information be classified at the proposed sensitivity levels?
4. Who is responsible for the protection of the information?
5. Who should have access to information and who should not?
6. What measures should be taken to manipulate information according to their level of sensitivity? (Raise key concepts)
7. What specific tools, practices and devices should be used to manipulate the information according to their level of sensitivity

1. Scope of the policy

Basically, the scope associated with this policy covers two aspects:

Affected team members: Take, for example, all the members of the team, only some of them (investigative journalism team, people in charge of handling complaints, etc.), even all the members of the organization or any external ally that somewhat collaborates on certain topics.

Types of data considered: Having as options only certain types of information handled by the organization or all the pieces of information handled by the group. This exercise is designed to consider the second case, however, it can be handled as best the group judges as long as the activity can be developed fluently.

It is suggested to discuss both aspects and put down the results of the discussion in section (1) of the template.

2. Sensitivity levels of information

What levels of sensitivity does the information handled by the organization have and how are they described? How can any piece of information be classified according to the sensitivity levels proposed?

1. Check the matrix of consequences of the activity data mapping and classification.
2. Introduce some types of information in classification schemes co- mmonly used in information security, then propose to keep up with impact levels developed

    - Public/confidential/secret/internal/regulatory data classifications, among others, are often used, taking into account the damage that may be caused by their commitment. In terms of our methodology, the same levels of impact proposed in previous sections can fill this space and therefore are suggested for reasons of simplicity

3. Unify in a single table cell the con- tent of each row by the level of impact developed and empty this information in the section (2) as shown in the graph 14.

Impact	Description its compromise might generate:
LOW	• Loss of public services in the office • Destruction or loss of equipment • Excessive administrative monitoring • Loss of small money or equipment
MEDIUM	• Destruction of office • Unmanageable workloads or stress • Break in • Trials • Prohibition of leaving the country • Excesive Fines • Loss of large amounts of equipment or money • Loss of the organization's website or social accounts
HIGH	• Data from complainants leaked • Death of beneficiary or member of the team • Traumatic events to members of the organization • Detention • Loss of legal status • Bankruptcy of the Organization • Loss of email accounts

Graphic 14. Levels of impact on information

3. Responsible for information

> Who is responsible for the data protection?

When handling information with different levels of sensitivity, it is important to ensure that security measures are put in place to protect data, so it becomes relevant to know who is responsible for implementing and maintaining the suggested security measures. Although standardized reference frames propose several figures regarding responsibility for information, it is recommended only to use the figure of the custodian of the information. Depending on the needs and dynamics of the organization, there are several approaches to determining who are the custodians of the information. E.g.:

- People who generate the information objects.
- Coordinators of departments or areas associated with information objects.
- People who manipulate the information at every moment.
- Specific people designated case by case.
- Other allocation criteria.

The idea is to present these options and discuss which of them best applies to the organization and write it down in section (3) of the template.

4 Restriction basis of access to information

> Who should have access to information and who should not?

In the framework of establishing data protection policies, it is important to consider the control of access to it by the team, this is achieved by having access control lists or rules that determine who can access each type of information and who does not Usually these considerations are included in a Data access policy, however, this type of policy is based on the principle of minimum privilege, where it is proposed that only people who need to manipulate certain information are able to access to it by rule, minimizing the possibilities of commitment.

The first premise that you want to validate with the group is if they would agree to formally follow this principle, it is expected that the agrees, but it is worth exploring any scenario where it might be difficult. In these cases, it must be made clear that the probability of compromising the information can go up considerably. The principle of the minimum privilege is written by default in section (4) of the template.

4a. Access control policies (optional)

In the event that the organization manages very sensitive information, is interested in deepening the control of access to information and the time is available, the first version of an access control matrix can be developed. In the section (4) of the template is an example of a matrix where different departments, areas, or even specific positions are placed as columns depending on the structure and dynamics of the organization, and as rows pieces of information with levels of high sensitivity, and then basically describe what areas or people can access to what pieces.

Information	Director	Complaint	Comunic.	Finance	IT
Data of complainants		X			
Reports	X	X	X		
Contributor's data	X			X	
Articles backup			X		X
Recording of sources			X		

Graphic 15. Data access control matrix

5. General data manipulation directives

What measures should be taken to manipulate information according to their level of sensitivity?

Using the matrix developed in the activity information flow, the general criteria described for each level of impact can be collected and depicted in section (5) of the template.

It is important that in this section you avoid describing specific tools or services, but the associated security features, which allow in case of changing any of them, have the criteria to select a new one that meets the same or better benefits. E.g.: do not suggest for communications Signal but Chat services with end-to-end encryption.

Impact	Considerations
Medium	Must communicate in encrypted services Must not be stored in equipment used by visitors or interns Its sending to external actors must be authorized by the custodian of the information There should only be physical copies under lock and key
High	Communicates only on end-to-end encrypted channels Only stored on devices with disk encryption Sending it to external actors is prohibited There must not be physical copies

Graphic 16. General considerations by level of impact

6. Specific data manipulation directives.

What specific tools, practices and devices should be used to manipulate the information according to their level of sensitivity?

In a similar way to the previous step, for each level of impact or sensitivity, devices, other resting places of the information and communication channels that were selected for each level will be collected, and thus placed in the template of section (6) as shown in the table. Space is left to place all necessary considerations that need to be met in each case if applicable.

For simplicity, if the organization and the facilitator consider it convenient, only the highest levels of impact can be considered, since the lower levels may require quite more time and effort to fill in the information requested in the template, in this case, the tables for low and medium levels can be deleted.

Highly sensitive data	
Device/communication channel	Considerations
E-mail	Only PGP or between Protonmail accounts
PCs	Only those with disk encryption
Cell phones	Strictly prohibited

Medium sensitive data	
Device/communication channel	Considerations
Chats	Signal, Wire, secret Telegram chats
Cell phones	With device encryption and password
E-mail	Between Gmail accounts
PCs	Using encryption of Veracrypt files
USB memory device	strictly prohibited
Physical support	In an office safebox

Graphic 17. Security directives by level of impact

_Aspects excluded in the policy

- Information lifetime: where is specified for how long the organization will retain certain types of information and what kind of processing will need to be done before deletion.
- Disposition of the information: how the information should be eliminated, according to its type of sensitivity, with the intention of avoiding reconstruction of this information or tracking of data.
- Detail of risks associated with this policy: where it is elaborated in what kind of risks are being attacked with the fulfillment of this policy.
- Specific responsibilities: where you can specify responsibilities that escape being the custodian of the information and may be relevant to the organization.
- Training plan on the concepts, techniques and tools proposed in the policy.

_References

R14 Information Classification Policy | ISO

03_ Acceptable use policy of devices, accounts and passwords

Estimated time: 60 min

_Justification

Currently, most organizations use technology within their processes, this technology inevitably has vulnerabilities and is prone to fail or be abused. Taking this into account, the idea of this policy is to provide safe use guidelines to the entry points of any member of the team, both at the level of devices and services on the Internet to protect the organization in the best possible way. Specifically, basic security measures in the use of mobile or desktop devices are described, widely used services such as email and social networks, the construction, and management of passwords and other means of authentication within the organization.

_Input data

- Data protection policy.
- Template 2: Acceptable use policy for computers, accounts, and passwords available in the physical or digital form to be filled in during the course of the activity.

_Associated Concepts

- Software updates: Partial code patches for the operating system that seek to improve functionality and correct new security vulnerabilities.
- Encryption: Ability to transform a message into something unintelligible for others, but also being able to revert it to the original content by those who must have access to the data.
- Disc or device encryption: Process that allows encrypting the entire contents of a computer's hard disk in such a way that it is only accessible and usable when a password or other authentication method is applied when switching on.
- Pirated Software: Any software that is installed out of the official channels without paying their licensing value.
- Malware: Any malicious software that executes actions on a computer without authorization from its owner or responsible party.

- Password: Sequence of secret characters that are used to enter a service or device.
- Credentials: the union of usernames and passwords, are given to identify a user. These credentials increasingly include other factors such as biometric aspects and temporary security codes.
- VPN (Virtual Private Network): Technology that allows treating equipment that can be in remote locations as part of an internal network, frequently used by organizations to unite in a single network several computers in dispersed locations. A particular application of this technology allows private users to encrypt the content of their Internet connections between their devices and places considered safe before reaching the Internet, they are generally used to protect surveillance traffic and access to blocked content.
- Tor: Network infrastructure that allows surfing the internet redirecting data by random points around the world. These data travel encrypted and the system is designed to provide anonymity and protection against surveillance.

- URL: Character sequences that allow locating resources on the internet, it means Universal Resource Locator. http: //sdamanual.org is an example of URL.
- Antivirus: Software that analyzes files in searching for known pieces of malware. They generally hold a database of previously identified threats, then com pare file by file with this database to detect any possible matches.
- PGP/GnuPG/GPG: A set of technologies that allow applying principles of asymmetric encryption (which is considered much more secure than traditional techniques) to messages and files in computer equipment. It is generally used as an advanced security strategy given the effort required for its implementation and the high level of security it provides
- Password Manager: Software that allows you to store previously designed passwords and recover them when needed. Generally they allow generating passwords with much greater length and complexity since it is not necessary to remember them at the moment of their use.
- Authentication in 2 factors or authentication in 2 steps: Authentication technique based on request to enter a service in addition to a password, another element related to something that the user physically possesses, such as a cell phone, a physical token, a card with codes, etc.

_Policies to be developed

- The Acceptable use policy, accounts, and passwords to be developed in this activity, abstracts existing contents in the following policies described in standardized reference frames:

- Equipment Acceptable Use Policy: Defines basic conditions for safe use of computers, telephones, and other mobile equipment. It usually deals with topics such as access passwords, computer lock, encrypt and incident reporting among others.
- Internet acceptable use policy: It establishes some security principles related to the use of browsers and other applications that connect to the internet in order to protect both equipment and data contained in it.
- Policy for acceptable use of electronic mail: Establishes specific guidelines for the use of electronic mail. In principle, it seeks to reduce phishing attacks, exfiltration of information and computer infections by malware, it may also include guidelines for the purposes in which mail, language, and other relevant aspects are used to a proper use of electronic mail in the organization.
- Social network acceptable use policy: Determines security measures to be taken in the use and administration of the organization's social networks. It usually has a set of general rules and other specific rules for each service of interest.
- Account and password policy: This policy establishes a set of rules that govern the creation, use, and maintenance of passwords in different services and access to devices, in case the organization manages some of its own systems, you can specify a password management guidelines for your users. Sometimes, this policy also considers aspects other than passwords, such as biometrics or other authentication factors.

_Guiding questions

1. What is the scope of the proposed policy?
   - Who does this policy affect?
   - Does it include equipment owned by the organization or any other equipment used to work on it?
   - Does it include computers or mobile devices?
   - What email and social media services are included?
2. Who is responsible for implementing and maintaining security measures in the equipment?
3. What are the general safety measures and directives on the management of equipment?
4. What are the general security considerations when using any communication channel?

5. What are the general security measures when using the internet?
6. What are the general security considerations to follow in the management of user accounts?
7. What security policies should be implemented with the services self-managed by the organization?
8. What are the security guidelines that should be followed when managing accounts with services hosted by third parties?
   - Email
   - Social networks
   - Other services
9. What security aspects should be considered around the management of passwords and other authentication mechanisms?

1. Scope of the policy

In summary, the scope associated with this policy covers the following aspects:

- To which people this policy impact: generally all members of the organization and allies who work on specific projects are included.
- What equipment this policy impact:
  - If there is only equipment include that is owned by the organization or if it also includes the equipment owned by the members of the organization used for professional purposes (work model Bring your own equipment or Bring Your Own Device - BYOD).
  - If it includes computers and/or phones and other mobile equipment.
- What type of digital services covers: whether it includes email, general internet use, social networks or any other service that is relevant to the organization. A valid option can also be all services that are used to work in the organization.

In this section, the contents of section (1) of the policy template for acceptable use of computers, accounts, and passwords should be discussed, modified and approved. It is very important that the provisions established in this and the other policies developed are aligned with the rest, in this case with the data protection policy which can provide help when deciding specific guidelines.

2. Equipment responsibility

> Who is responsible for implementing and maintaining security measures in the equipment?

Discuss, modify and approve the content of section (2) of the policy template for acceptable use of equipment, accounts, and passwords that deals with the ownership of the equipment and the responsibilities for using them and reporting incidents.

- The most notable variation in this step depends on whether the organization has its own equipment, all the equipment are owned by the members of the organization (BYOD) or a mixture of both modalities. In the template, there are several examples that can be reduced to the particular case of the organization executing the activity.

3. General equipment use

> What are the general safety measures and directives on the management of equipment?

Discuss, modify and approve the content of section (3) of the policy template for acceptable use of computers, accounts, and passwords. Some of the most important aspects discussed in this section are:

- Authentication means for equipment such as passwords or biometrics.
- Blocking equipment when left unattended.
- Sharing credentials for equipment access.
- Operating system updates.
  Use of pirated software.
- Considerations against malware infection.
- Disk encryption.
  - On computers.
  - On cell phones and
  - other mobile devices
- Use of equipment for purposes other than the work of the organization.
- Use Antivirus and Antimalware.

Equipment Acceptable Use Directives

Discuss, modify and approve the section of directives in section (3) of the corresponding policy template. It is ideal that the group has prior knowledge of specific security issues, being the optimal case to have this discussion after the completion of a digital security workshop, and as each aspect worked in this manual is covered, you can discuss how to implement this concept or tool to the corresponding policy. Take for examples those listed in the template that can be used as they appear, edited or eliminated are, among others:

- The mandatory use of user passwords on computers and cell phones used to address sensitive issues of the organization. These passwords must comply with the password policies at the end of this document.
- The mandatory use of screen protectors that block users of computers and cell phones after a certain period of inactivity.

- The implementation of system encryption: in the case of mobile devices this feature is often activated by default and in the case of computers it may require time, knowledge and special effort to implement an effective disk encryption. In this aspect, it is common to concentrate efforts on those computers that handle highly sensitive data, on equipment maintenance plans that consider the configuration of this disk encryption or on the use of operating systems that facilitate system encryption by design.
- The policy of operating system updates: It is generally considered as the minimum necessary to make automated security updates, from that point on it is possible to adjust the policy to each organization according to specific needs.
- Use antivirus and antimalware software, being able to specify specific approved software or selection criteria.

4. About the use of any communication channel

> What are the general security considerations when using any communication channel?

Discuss, modify and approve the content of section (4) of the corresponding template. Some of the most important aspects discussed in this section are:

- The handling of highly sensitive data through these channels and towards external stakeholders of the organization.
- Use of equipment for purposes other than work related to the organization.
- The attitude of the organization's members when using official communication channels. Attitudes regarding discrimination, harassment, spam, etc. in the communication channels used for organizational purposes.
- Provisions on the use of the equipment to carry out actions that violate the intellectual property rights and copy or distribute material protected by copyright.

5. Internet general purpose directives

> What are the general security measures when using the internet? Discuss, modify and approve the content of section (5) of the corresponding template. In case some consideration does not apply to the organization, it can be eliminated without any consequence. Some of the most important aspects discussed in this section are:

- The use of circumvention and anonymity instruments on the internet when using computers such as Virtual Private Networks (or VPNs in English), Tor or other similar tools. Normally these measures are associated with levels of sensitivity of the data handled. Since it is a directive, it can be specific in approved point tools or selection criteria.
- The prohibition of activities that unjustifiably deteriorate the quality of the connection (for example, downloading torrents or streaming content not related to work).

Strategies against identity theft

Given that the most frequent attacks on organizations today are largely related to phishing attacks, it is important to specify clear strategies to face these risks. It is proposed to review in section (5) of the template in use the corresponding section and discuss, edit, add and approve some of the proposed strategies, related to topics such as:

- Knowledge throughout the organization of the official communication channels of the relevant stakeholders (e.g. Suppliers, staff, public institutions) and avoid any communication or exchange of sensitive information through different channels. (Email addresses, accounts in social networks and telephone numbers among others).
- The management of communications that request sensitive data such as credentials, banking, and personal information, as well as the development of a series of indicators that help detect possible cases of identity theft.
- The development of rules for handling suspicious attachments

6. Account management

> What are the general security considerations to follow in the management of user accounts?

Discuss, modify and approve the content of section (6) of the policy template for acceptable use of computers, accounts and passwords. Some of the most important aspects discussed in this section are:

- Obligation of individual or shared accounts.
- Responsibility for the use of own accounts.
- Implementation of the principle of minimum privilege in the creation and configuration of user accounts.
- Management of account recovery mechanisms.

7. Management of accounts in self-managed services (internal systems, hosted websites, servers, etc.)

> What security policies should be implemented with services self-managed by the organization?

Discuss, modify and approve the content of section (7) of the policy template for acceptable use of computers, accounts and passwords. Some of the most important aspects discussed in this section are:

- Concept of administrators: who creates, monitors, controls and eliminates an account and under what circumstances ?.
- Who authorizes the creation of the accounts.
- Avoid administrative accounts for daily use.
- Non-disclosure agreements (NDA).
- System access roles.

8. Directives on management of accounts in third-party services (e-mails, social networks, collaboration services, etc.)

> What are the security guidelines that should be followed when managing accounts in services hosted by third parties?

Discuss, modify and approve the content of section (8) of the policy template for acceptable use of computers, accounts, and passwords. Some of the most important aspects discussed in this section are:

About the email

- Publication of personal opinions in the emails.
- Opening of suspicious attachments.
- Generation of unwanted or malicious mail.
- If required in the data protection policy consider mail encryption

About other third-party services

- Who manages the access credentials.
- Use of collaborative publishing tools that protect the credentials of social media accounts.
- Use of password managers.
- False accounts monitoring if applied

For each specific service

- What characteristics can be configured in addition to those present in the general policy?

For example: Facebook

- Use of pages vs users or groups.
- Management of administrators.
- Security notifications.
- Authentication in two factors.
- Emergency contacts.

For example: Twitter

- Linking phone number to the account.

9. Password and authentication policies and directives

> What security aspects should be considered around the management of passwords and other authentication mechanisms?

Discuss, modify and approve the content of section (4) of the corresponding template. Some of the most important aspects discussed in this section are:

- The basic principle of direct responsibility in the use of accounts, devices or services with a password in their care.
- Security measures for the creation of passwords, in subsequent steps these measures will be defined in detail.
- General security practices for passwords.
  - Repetition of passwords.
  - Existence of physical copies.
  - Remembering of passwords in browsers.
  - Use of password managers.
  - Passwords sharing.
- Policy proposals for passwords and authentication.
  - Length.
  - Complexity
  - Dictionary.
  - Contents to avoid in the construction of the policy.
  - Authentication in several factors.
  - Use of password administrators.
  - Access passwords on mobile devices.

Aspects excluded in the policy

- Remote management of equipment.
- Monitoring and auditing compliance with security policies in teams.
- Explicit prohibition of network monitoring, port analysis and use of honeypots and honeynets.
- Explicit prohibition of execution of any illegal task, for example denial of service attacks (DoS and DDoS) and blocking of access to resources to other users without justification.

_References

R15 Acceptable use policy template | SANS Institute

R16 Sample Acceptable Usage Policy | getsafeonline.org

R17 Email policy template | Sans institute

R18 Password Protection Policy template | SANS Institute

04_ Clean desk policy

Estimated time: 20 min

_Justification

In any kind of organization, it's natural to arrange large amounts of highly sensitive information in the paper. On the other hand, when we talk about digital workspaces the equipment used to store and manipulate data, becomes an object of interest to those who might want somewhat compromise the organization. The idea behind this policy is to establish a set of strategies to ensure both the physical information and the integrity of the equipment. This policy is one of the most linked to daily basis tasks since it considers activities that must be carried out during the entire working day.

_Input data

- Template 3: Clean desk policy available in the physical or digital form to be filled out during the course of the activity.

_Policies to be developed

The initial intention is, the Clean desk policy is explicitly found in most reference frames used in various organizations.

_Guiding questions

1. What is the scope of this policy?
2. What measures should be taken in the organization's workspaces?
3. How should physical information be handled in workspaces?
4. How should physical information be available once is dismissed?

Scope of the policy

In summary, the scope associated with this policy, available in section (1) of the clean desk policy template, covers the following aspects:

- Workspaces affected by this policy.
- A person affected by this policy.

Measures in spaces with work equipment

What measures should be taken in the organization's workspaces? Discuss, modify and approve the content of section (2) of the corresponding template. Some of the most important aspects discussed in this section are:

- Particular steps to follow at the end of the workday.
- Management of unattended equipment during the workday.
- Use of a physical shield mechanism for devices in workspaces

Management of physical data in workspaces

How should physical data be managed in workspaces?

Discuss, modify and approve the content of section (3) of the corresponding template. Some of the most important aspects discussed in this section are:

- Processes to follow at the end of the day to keep the workspaces free of sensitive data.
- Management of filing cabinets or other physical data shield mechanisms.
- Management of furniture keys and safety boxes.
- Existence of sensitive data in workspaces.
- Management of paper in printers.
- Management of information on blackboards and billboards.
- Management of portable digital storage devices.

Physical information layout

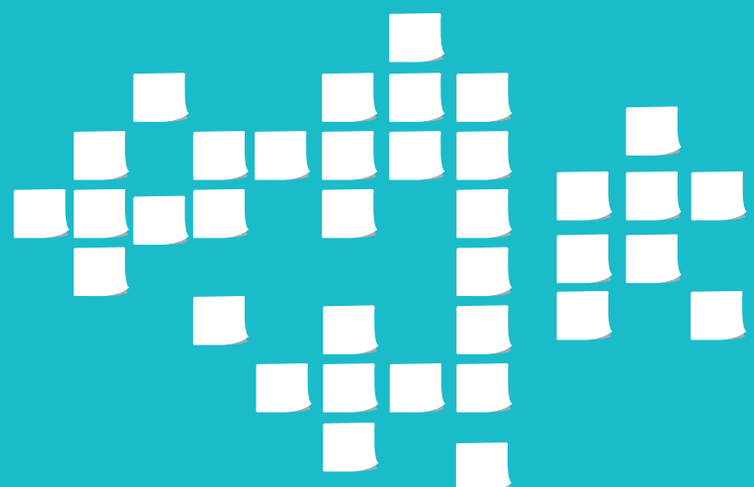
How should physical data be managed in workspaces?

Discuss, modify and approve the content of section (3) of the corresponding template. Some of the most important aspects discussed in this section are:

- The use of equipment or techniques to make unintelligible physical information.
- To secure places by depositing information in physical after it has been processed for its disposal.

_References

R19 Clean Desk Policy template | SANS Institute



03_ Threat model and Procedures

_ Definitions

- Threat:
  Possible event or event with negative consequences.
- Risk:
  The possibility of a threat to materialize.
- Vulnerability:
  The condition of weakness or the existence of a measure that protects something from a threat.
- Security incident:
  Any violation of security policies or violation of a given resource.
- Security procedure:
  A series of steps that can be followed in order to face a security incident.
- Succession plan:
  List prepared prior to a security. incident where those responsible for complying with the security procedure are specified and who would supply them in the event that the first ones are not available.
- Communications plan:
  Compilation of contacts that the organization wishes to hold in the event of a certain security incident. Including with which stakeholder communication will be established, which members of the organization are responsible for these communications and what should be communicated.
- Evidence:
  Any physical or digital element that can be used for future investigations and at the same time can be considered evidence for legal and / or criminal actions.

01_ Risk matrix

Estimated time: 120 min

_Justification

The idea of this activity is introducing the concept of risk analysis of the organization and also to use an abstraction of the risk matrix methodology to make a first analysis of the organization's security context, which will be used to select security scenarios in order to elaborate procedures to the case in the second activity.

_Input data

- Levels of consequences developed in activity data mapping and classification in section 01

_Products

_Direct

- List of possible threats to the organization prioritized by possible impact and probability of occurrence estimated by the team.

_Indirect

- Better understanding of possible adverse scenarios through which the organization might undergo.
- Better criteria for collective categorization of possible threats.
- Better criteria of prioritization of potential threats and establishment of security controls.

_Previous planning

In case of carrying out the activity in digital, it is suggested to have a spreadsheet or other software with all the necessary fields and formats.

_Materials

In case of doing the activity on paper:

- Post-its or sticky notes and markers or
- Large pieces of paper to stick on the wall and markers.

In case of doing the activity in digital equipment:

- Computer.
- Projector.
- Spreadsheet ready to fill, showing the headings with stakeholder categories.

_Instructions

1. Introduce to the group the concept of threat (Possible negative event occurred to a given resource), considering the following aspects:

- These can occur by human and non-human causes (natural disasters, spontaneous reactions, wear and unscheduled malfunctions, etc.).
  These can be intentional or accidental.
- These can be provoked or fortuitous.
- These can affect physical, digital, human, legal and administrative resources among others. In fact, many organizations consider the affectation of their image and positioning as a resource, being a valid consideration within the exercise.

In general, it seems easier for participants to use a structure in the wording of threats similar to these:

› [Something is wrong]

A. Absence of the director.
B. Thieves break in the office.

[Something bad happens to some resource or stakeholder linked to the organization]

A. The twitter account has been hacked.
B. Access to the bank account is lost.

However, sometimes this way of building threats can be so vague that they do not represent possible events, but other things such as vulnerabilities or lack of security measures. In this regard, facilitators are recommended to ensure that the wording of threats throughout the exercise corresponds to events. If the facilitator deems it appropriate, a drafting structure can be proposed that helps reduce errors, for example:

[A stakeholder] [execute an action] to/about [a resource] [provoking certain consequences – optional]

A. A hacker introduces a malware into the computer of the organization's director.
B. The intelligence agency of my country monitors telephone calls from journalistic sources exposing the physical integrity of those.

[An event] [make an action] to/about [a resource][provoking certain consequences – optional]

A. An earthquake measuring 7.5 on the Richter scale or more occurs, destroying the data center of the company where the website is hosted.
B. A blackout leaves the office without electricity, making it impossible to work on computers.

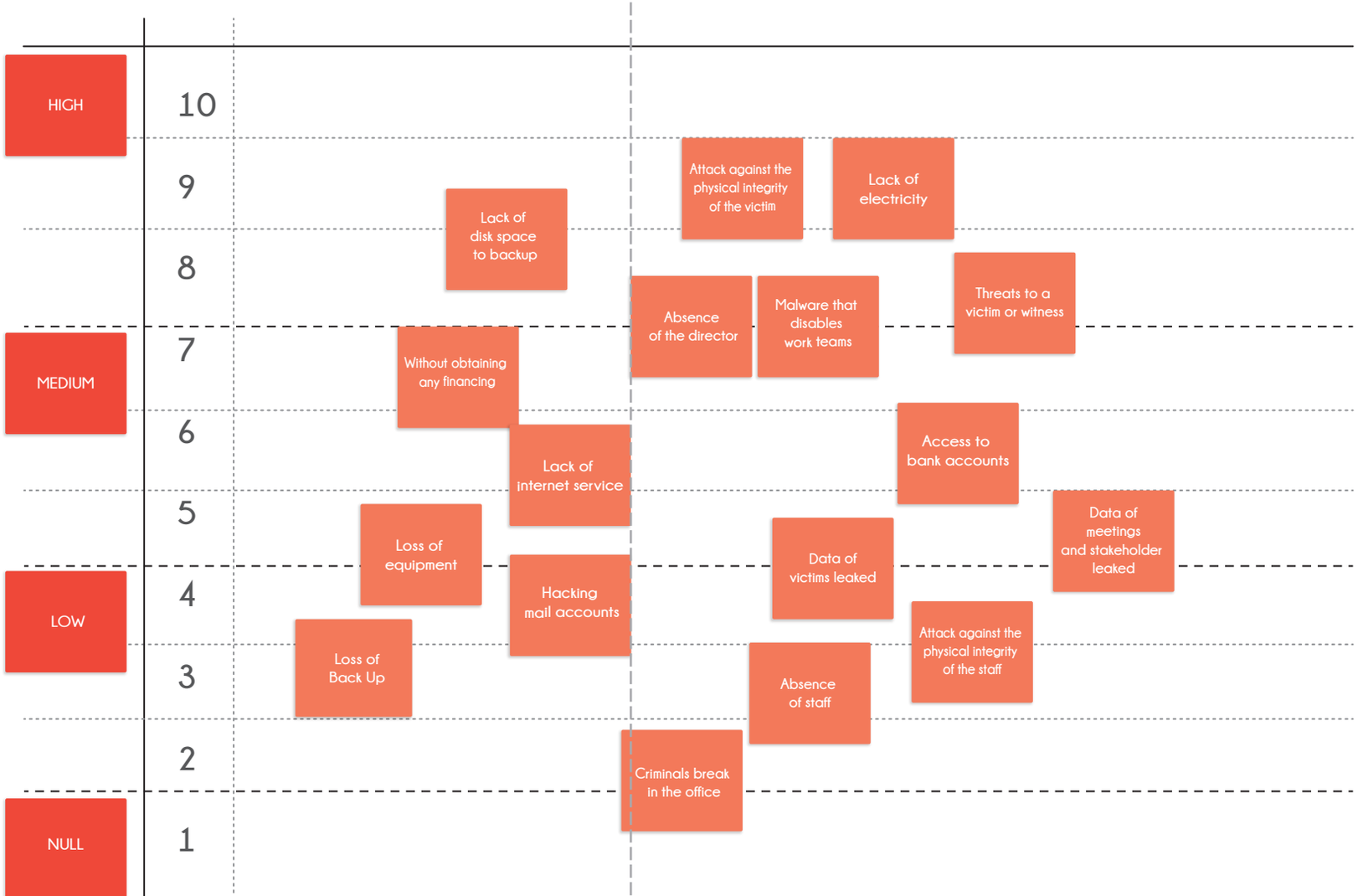
This wording can be adapted to consider threats without adversaries or clear events, as well as any other variation of threats that do not directly cover these drafting proposals.

2. Ask the participants to think about threats to the organization, take note and place them visible for everyone.

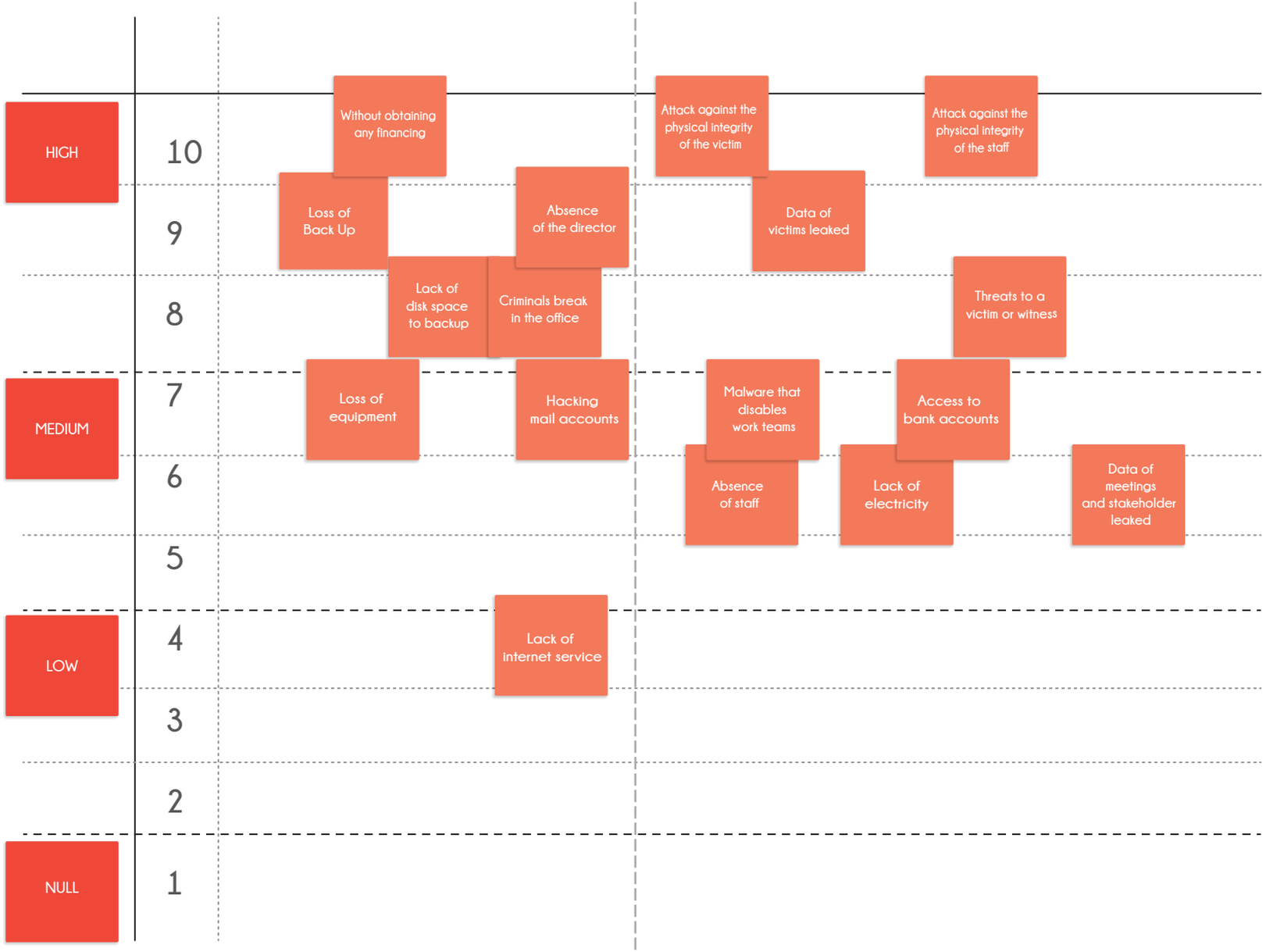
Graphic 18. Map of threat.

3. With all the threats in one place, use levels of impact development in the activity Data mapping and classification and place them as the vertical axis of a matrix, then along with the help of participants assign each threat a level of impact locating the sticky note or equivalent to the height of the selected impact level.

- It is also suggested to place the qualitative impact levels defined above, then put a numerical scale as shown in the graph. This can help quantifying the level of risks after completing the activity.



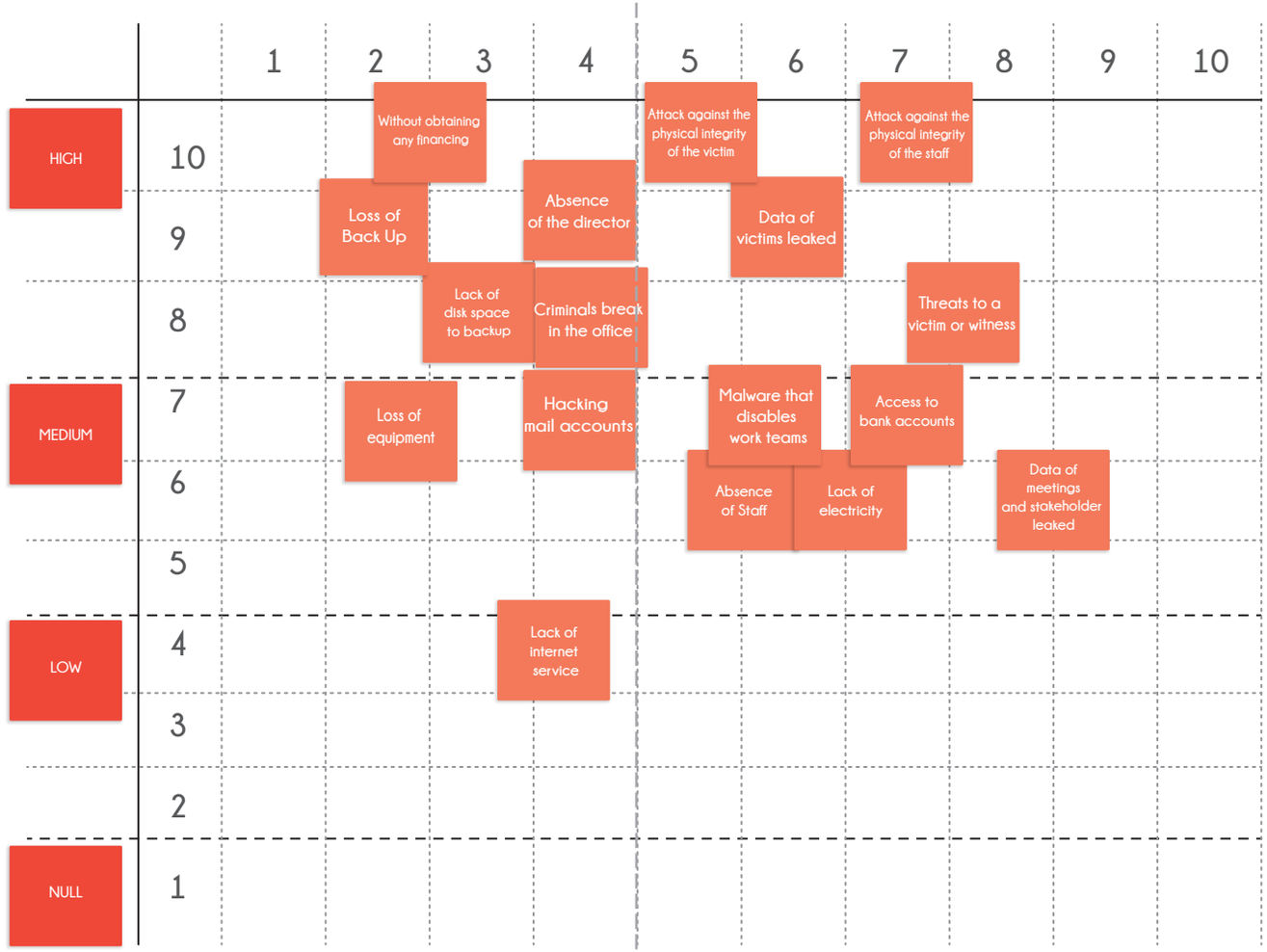
Graphic 19. Map of threat adding impact level



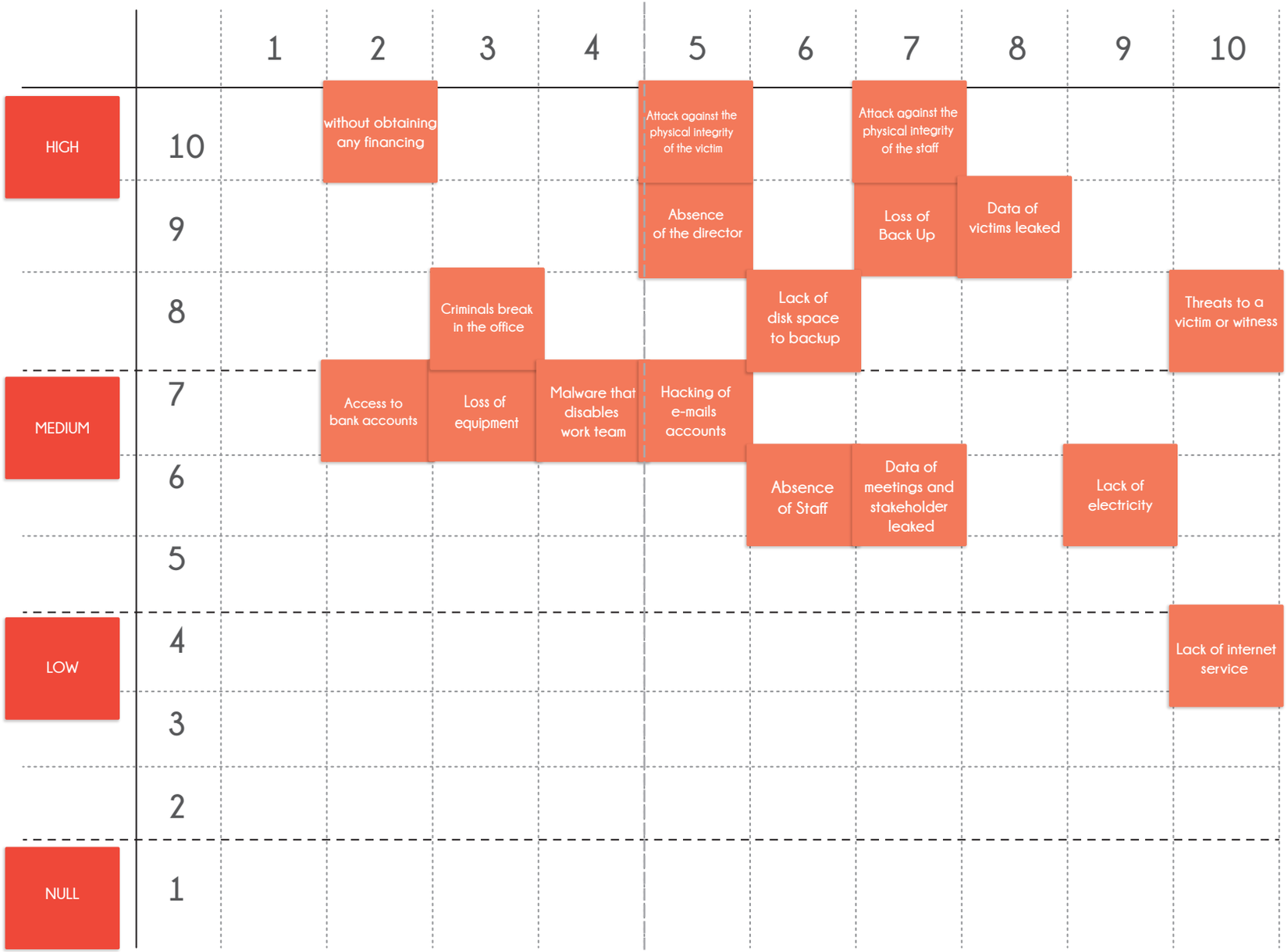
Graphic 20. Reorganizing threats after impact levels

4. Explain the concept of occurrence probability and define a scale to represent it onto the risk matrix. Reorganize the threats on the horizontal axis with the help of the group in such a way that they coincide not only with the impact scale but also with the probability of occurrence selected in each case, completing the risk matrix of the organization, as shown in graphic.

- In the graphics a scale of 1 to 10 is suggested, this can be changed by another type of scales such as those described below. However, if you want to make a numerical analysis of the threats it is necessary that the scale be also quantified in numbers and equal to the scale used for the risk levels.
  - Low, medium and high probability
  - Null, low, high probability and certainty of occurrence.
  - Scale from 1 to 5.



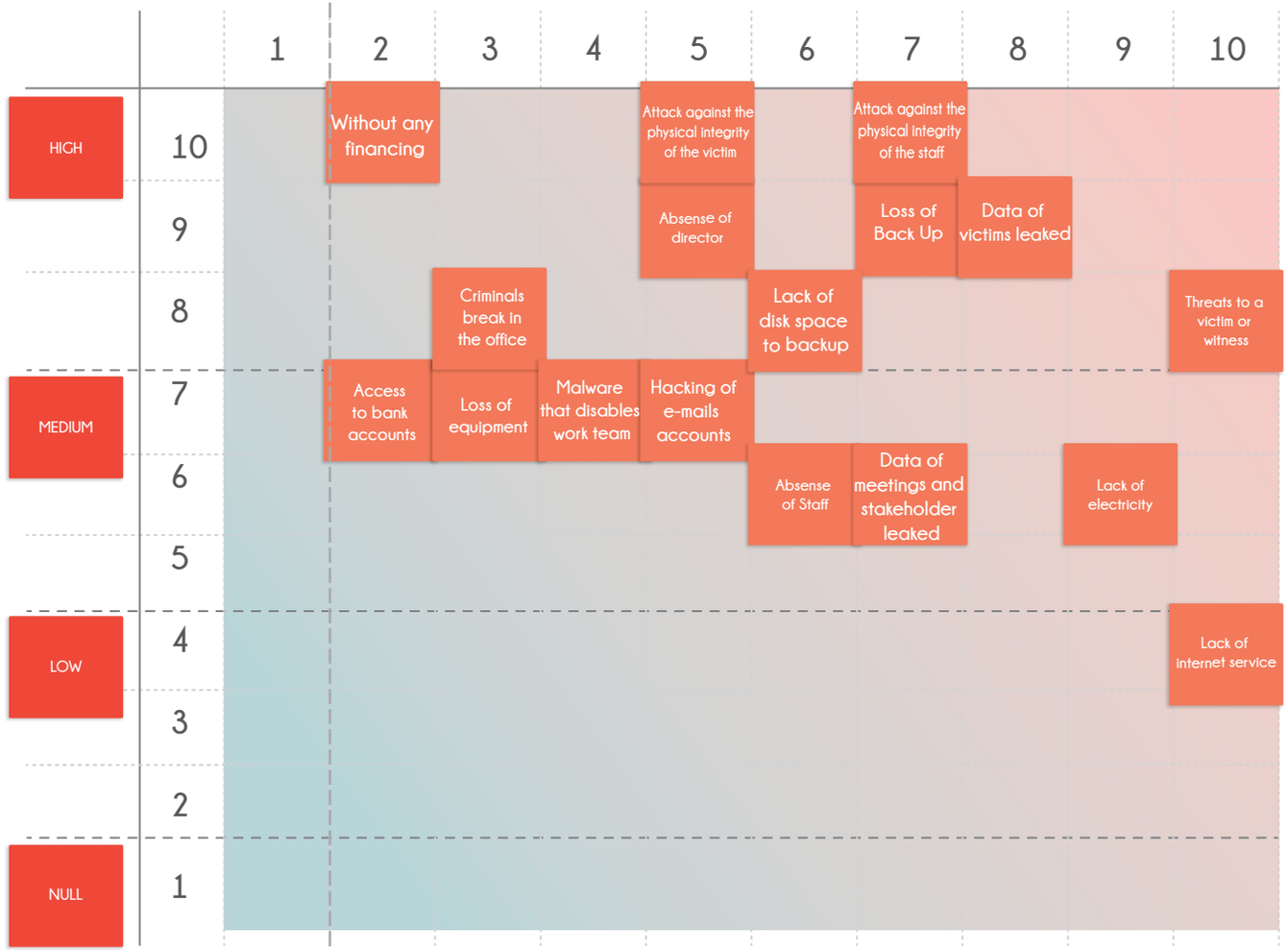
Graphic 21. Threat map adding the probability levels of occurrence



Graphic 22. Reorganizing threats post probability levels of occurrence.

5. Discuss levels of risk present in the matrix and read the security context of the organization through this tool.

- It is essential that participants come clear that hthe most important threats to attend must be those that have high levels of impact and associated high probability of occurrence (in this case those closest to the upper right corner of the matrix).
- In case of wanting to perform a quantitative analysis of the risk levels, when previously has been used numerical scales in levels of impact and occurrence probability, it will be enough to multiply these values for each threat and then organize the results obtained from highest to lowest (risk levels).
- This exercise results in a subjective analysis by the members of the organization, and for no reason represents a rigorous and accurate analysis of the risk context of the organization. Even if the same team repeated the activity the next day it could result in a different risk matrix.
- This risk matrix, as well as any other input that represents the risk context of the organization, is a temporary input that does not consider risks to change over time. It is very important to emphasize with the participants that this matrix represents "a picture" of the state of risk for that particular moment, and the invitation is to repeat this exercise periodically to update this obtained representation.



Graphic 23. Risk matrix analysis

_Closure of the activity

At the end of the activity you can discuss and emphasize what has been achieved:

- Criteria for the detection of threats were defined, and a map of current threats proposed by the team was made.
- Criteria for the study and prioritization of threats were developed. These criteria were also used during the exercise of threats mapping.
- A risk matrix building methodology was introduced, and it can be replicated in the future of the organization.

_References

R20 SAFETAG

R21 Saferjourno

02_Introduction to security procedures

Estimated time: 60 min

_Justification

The idea behind this activity is to complement policies revealed previously as preventive strategies along with the development of procedures to be applied during security incidents such as reactive strategies pursuing to mitigate impact of threats once they have been implemented. Specifically, this activity seeks to abstract the concepts of procedures, training, communications plans, succession plans and arrangement activities in a single dynamic serving as an introduction to the area of incident response developed in the information security literature.

_Input data

_Risk matrix.

_Products

_Direct

- Initial security procedure for one or two selected scenarios.

_Indirect

- Instruments to develop any other security procedure missing from the organization.
- Better understanding of the relevance of internal, external communications and the succession of responsibilities during attention of security incidents.

_Previous planning

In case of carrying out the activity in digital, it is suggested to have a spreadsheet or other software with all the necessary fields and formats.

_Materials

In case of doing the activity on paper:

- Post-its or sticky notes and markers or large pieces of paper to stick on the wall and markers.

In case of doing the activity in digital equipment:

- Computer, projector.
- Spreadsheet ready to fill, showing the headings with stakeholder categories.

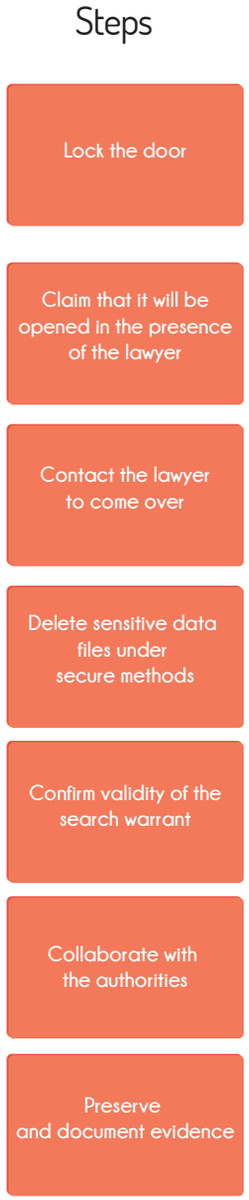
_Instructions

1. Check risk matrix raised in the previous activity and select one or two threats considered relevant to raise security procedures.

- It is natural that there are threats depending highly on the personnel or external allies for their resolution, although it is desirable they are resolvable threats to a greater extent by the same members of the organization.

2. For each threat, which from now on will be treated as security incidents since procedures for its occurrence will be prepared, make a brainstorm of actions that should be taken as steps, write down each one on sticky notes, put them on paper or onto the wall, then reorder as new steps are added. As an aid to the group, usually actions taken in a procedure follow:

- Minimize the damage.
- Clean remaining artifacts from the incident.
- Resume activities as soon as possible



Graphic 24. Steps for the procedure

3. For each step ask the group who would execute the procedure. Write down on a sticky note and place it in a second column on the wall next to the step in issued, you also can ask the group who would supply this responsible person in case that is not present during the incident. If applies, take note and place these substitutes below the principal responsible as shown in the graph.

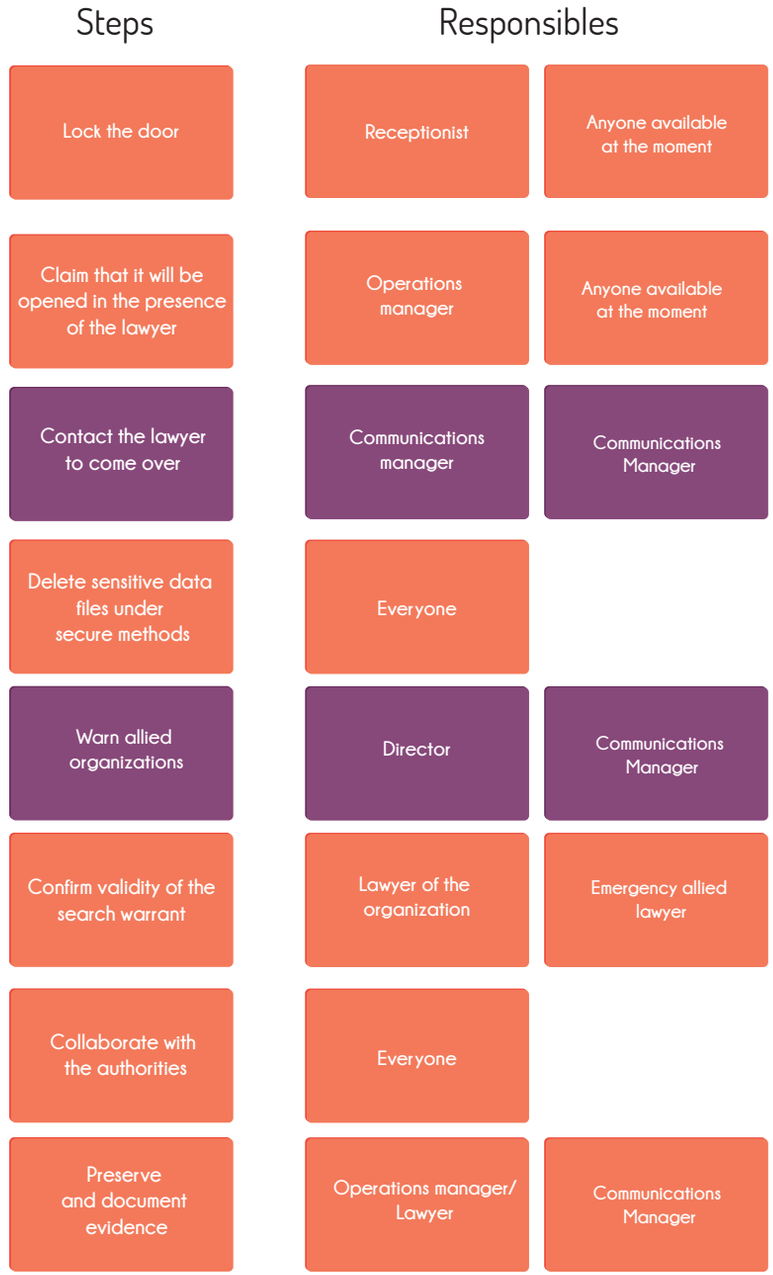
Graphic 25. Responsibles for each step

4. With consent in the group on the steps of the procedure to take, ask at what point should establish communication with the organization's external stakeholders. The idea behind this is to write down these mentioned communication points as new steps (ideally in a different color) in order to include them into steps of the procedure by rearranging the existing ones.

- These communications are normally mandatory or highly desirable to resolve the incident, such as networks of allies, external suppliers, etc.

- It is possible that in the same dynamic of the activity, this communications map developed in step 2 has been advanced naturally. In that case, by completing any missing communication and continuing would be enough.

- For each step related to external communications, verify that it always appears who would be contacted, either in the step or in the person in charge.



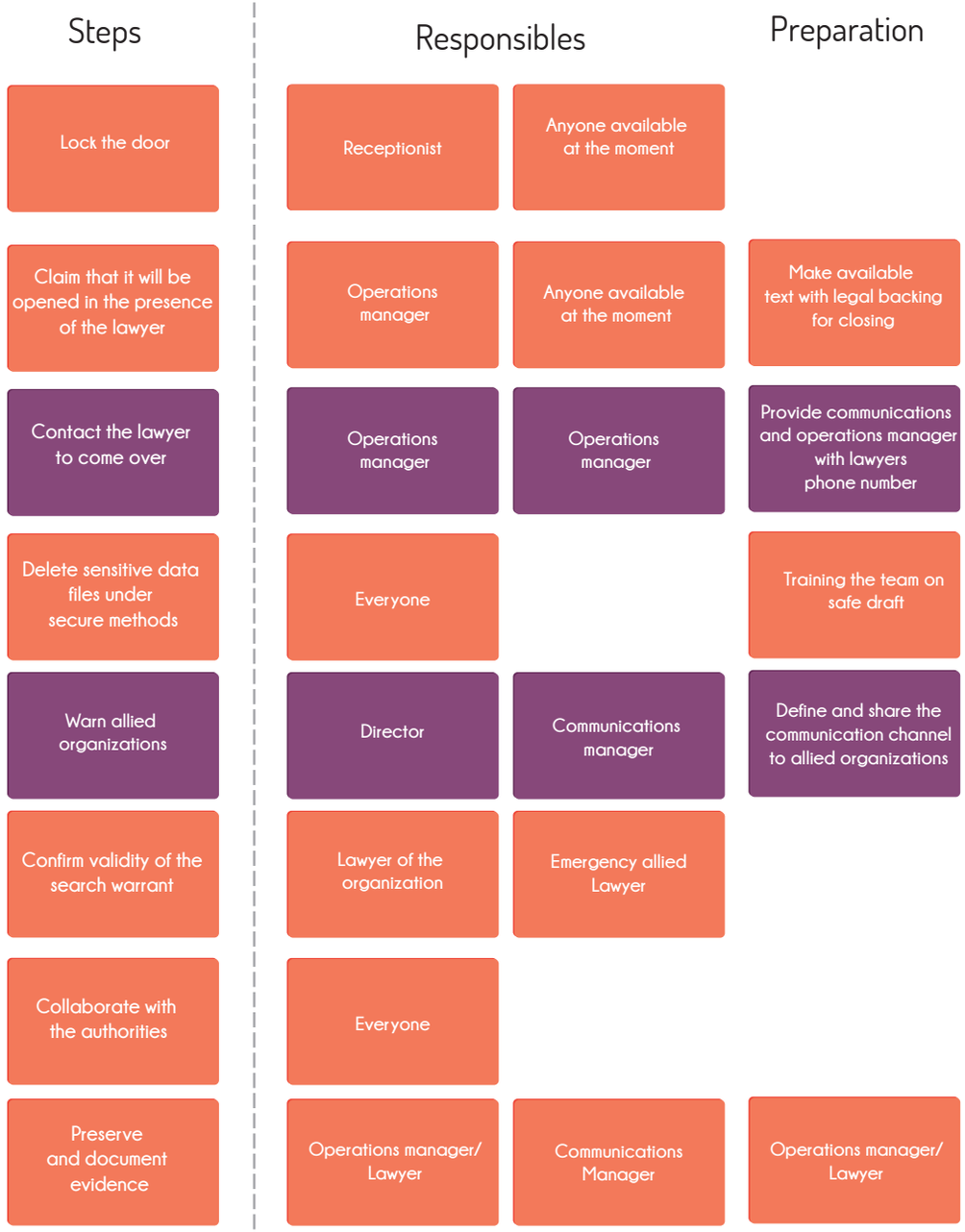
Graphic 26. Steps to the communication plan

5. Create a third column with the heading "requirement" and for each step ask the team What do I need to guarantee BEFORE the incident occurs so that this step can be fulfilled?. Take note of each requirement on a sticky note and place it next to the corresponding step, it is natural that some steps have no associated requirement actions. Some common examples of requirement are:

- That A has the contact of B external consultant.

- C knows how to turn off the internal server.

- Everyone knows how to erase information safely.

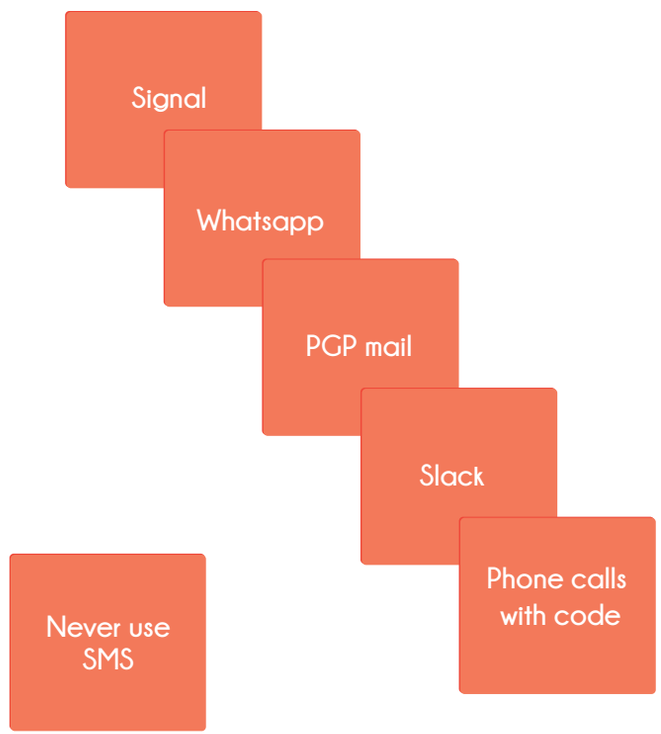


Graphic 27. Previous preparation for the procedure

6. Discuss with the group How would they communicate with each other during the resolution of the incident? Guide the discussion about which channels are considered safe and reliable to keep the group informed during the incident, as well as which ones would be used formally during this one type of incident. It is suggested to take note of these channels and list them in order of priority in case the first one fails during the incident.

- It is worth remembering that different incidents can affect different communication channels.

7. Suggest the team to empty the information collected during this activity in a formal document. You can use the template 4 available on the website of this material (https://sda.guerracarlos.org).



Grafic 28. Internal communication order

_Closure of the activity

At the end of the activity you can discuss and emphasize what has been achieved:

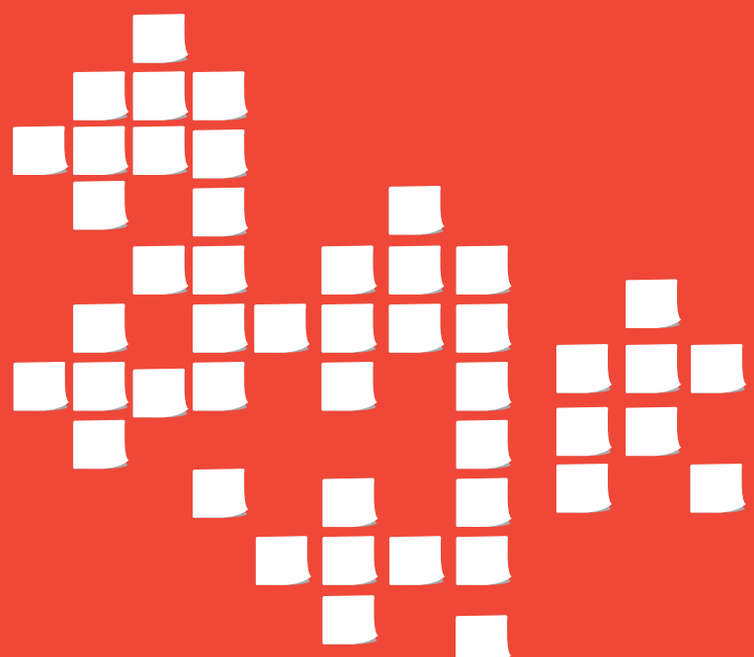
- Real procedures were developed for specific incidents.
- Steps of the procedure were associated with responsible personnel and successors.
- External communication plan procedure was integrated.
- Internal communication bases were established during incidents.
- Steps to build security procedures with methodology were explored.

After the activity is over, it is worth proposing to the group subsequently any incident happened, to hold a subsequent meeting where the team will at least ask the following questions:

- What happened and at what time?
- How well did the team respond to the incident?
- Were the procedures followed? Were they adequate?
- Were there steps or actions taken that inhibited the recovery of the incident?
- What would the team do differently if something similar happens in the future?
- What corrective actions can prevent similar incidents in the future?
- What indicators should be revised in the future to detect similar incidents?
- What instruments or resources are needed to analyze, detect and mitigate future incidents?

_References

R22 Umbrella: security made easy - Android App I Security First
R23 Digital First Aid Kit - Kit de primeros auxilios digitales
R24 AccessNow Digital Security Helpline - Línea de ayuda en seguridad digital



04_ Closure

01_ Conclusion

After executing the activities proposed in this manual, we will have equipped the organization with criteria and instruments to begin a coherent and robust security plan. It is important to highlight that the policies and procedures developed in this manual represent just a first approach to the development of a formal security plan and as long as the organization feels comfortable, it should be deepened and complemented with other aspects and strategies that cover the missing spaces in the proposed methodology.

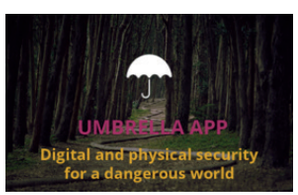
In addition to developing formal policies on organizational security, it is recommended to consult references on information security and complement the development of policies and procedures with the generation of a safety training plan for the entire team of the organization. This training process can help to maintain in a more effective way the policies and procedures developed as well as an adequate integration of security principles in the daily processes of the organization.

Below are some projects of interest to security facilitators for organizations, which in addition to serving as inspiration and input for this manual, are complementary references to expand the scope of security work that can be carried out by an organization that works on activism or any other form of advocacy in the area of Human Rights:

02_ References

Holistic Security | Tactical Technology Collective
Manual that addresses activities to explore the state of the security of the organization from an integral point of view (digital, physical and emotional), as well as collaborative activities to generate strategies against the most relevant detected risks. Uses a narrative of knowledge construction through facilitation.
https://holistic-security.tacticaltech.org

SAFETAG | Internews
Complete methodology for the evaluation and proposition of road maps for the resolution of vulnerabilities and confrontation of threats for organizations that carry out activism.
https://safetag.org



Umbrella
Android application with training material in strategies against physical, digital and emotional security risks, contain checklists proposed in specific situations.
https://secfirst.org

Digital First Aid Kit | Digital Defenders Partnership
Set of quick response guides to frequent security incidents.
https://rarenet.github.io/DFAK/es/

Security Education Companion | Electronic Frontier Foundation
Set of resources for facilitators in digital security and privacy issues.
https://sec.eff.org

Surveillance Self-Defense | Electronic Frontier Foundation
Set of quick guides on digital security issues and risk analysis for people doing activism.
https://ssd.eff.org

Security in a box | Tactical Technology Collective - FrontLine Defenders
Set of training guides on issues of information security aimed at human rights activists, it is useful for executing training plans, review policies and security considerations for policies.
https://securityinabox.org/en/

Me and my shadow - Training curriculum | Tactical Technology Collective
An instrument for building training programs in digital security along with concepts and associated.
https://myshadow.org/train