TRAIN FOR TRADE

UNITED NATIONS
UNCTAD

# Special Course on Building Port Resilience Against Pandemics (BPR)

## Participant manual

### Section 3: Technology Preparedness

Strenghtening Knowledge
and skills through **innovative approaches**
for sustainable economic development

Development Account
Department of Economic and Social Affairs

Irish Aid
Government of Ireland
Rialtas na hÉireann

learn.unctad.org

# Table of Contents





Cover photo: Tom Fisk / Pexel

# 3. TECHNOLOGY PREPAREDNESS

Technological resources (applications, processes, information and communication systems) are usually designed for use in normal circumstances and conditions. Here are examples of design decisions that are usually taken under normal circumstances:

- The main business information systems are made accessible only at local level (from the office via the corporate local area network, LAN) for confidentiality and security reasons.
- Although much progress has been made and continues to be made in the digitalization and elimination of paper in the search for greater efficiency and respect for the environment, there are still many processes that have not yet been digitalized. In normal circumstances, the digitalization of these paper processes is considered important, but not urgent.
- In most cases, it is not considered necessary to implement collaborative, videoconferencing and teleworking tools due to the on-site presence of the port workforce.
- The on-site working mode means that generally the information technology (IT) resources that are made available to the users are fixed devices (desktops) due to their low cost/performance ratio.
- The communication lines (internal, external and internet) are sized and secured taking into account the information flows (and bandwidths) that are required when most employees are working on-site.

All these design decisions may no longer be valid in a pandemic situation and may need to be reconsidered, redesigned and reprioritized. This will be covered in this section as well as what is needed to prepare technological resources to cope with a pandemic situation.

The objectives of this section will be to:

- Identify appropriate technology solutions for alternative work arrangements;
- Plan paperless transition;
- Identify and implement effective digital communication tools.

## 3.1 Teleworking technology, capacity and security

Technological resources have been designed under normal circumstances, where the organization's personnel usually carry out their tasks in person from the workstation made available to them and which includes the necessary technological devices (personal computer or tablet, printer, etc.). In a pandemic situation, where people may have to remain isolated in their private homes, organizations have to make sure that the necessary resources are available remotely and offer sufficient capacity.

In a lockdown situation, it is necessary to check and adapt the technological resources so that:

- Personnel have the necessary resources to access business information systems remotely

It must be ensured that all personnel who work remotely have the necessary and sufficient means to do so. Minimum requirements should be a PC and an internet connection available at the location from which they are going to work (e.g. their home).

As a first step, it is advisable to draw up a list of the personnel who would be teleworking and from where:

- √ The port's IT department identifies which employees currently have a laptop that would allow them to work remotely.
- √ Each employee must indicate whether they have their own equipment (PCs) and a WIFI or 4G/5G broadband internet connection at the location where their remote workstation would be located.

**Single computer policy**

It is recommended that the port provides PCs to ensure they are equipped with the corporate security mechanisms and measures (e.g. antivirus, security patch update policy and necessary for safe connection to the information systems). For this reason, it is advisable to acquire the necessary devices to equip those employees who do not have them as well as to take into consideration the implementation of the "single computer" policy in the organization.

To date, most organizations have provided employees with a work computer (PC) at their usual work station, complementing it with a portable computer (PC) only for those who needed to be mobile due to the requirements of their job . In a pandemic situation, the mobility requirement is extended to the whole (or most of the) port workforce. It is no longer necessary (except in very rare cases) for a user to have two computers. This is the meaning of a single computer policy: the organization provides each user with only a laptop.

The cost/performance ratio is still better for desktop PCs than for laptops, but the gap is closing. This, together with the need for mobility in the event of a pandemic, greater security of corporate equipment and a reduction in hardware and software costs compared to maintaining two computers, makes the single computer policy something worth considering and implementing in the organization.

In cases where employees have a personal laptop rather than a company laptop to carry out teleworking tasks, the equipment will have to meet some minimum requirements:

- √ Have the latest operating system and security updates installed;
- √ Have an updated antivirus installed.

In addition to the hardware (PC) every user should have a WIFI broadband internet connection. If not, 4G/5G ad-hoc connections will have to be acquired, or the organization must check whether the employee has a corporate/personal mobile phone with a data plan that allows data to be shared with a computer and used as a 4G/5G connection.

In addition to the PC and the internet connection, it is important to make sure that the users have the necessary equipment to be able to telework. For example, for organizations which implement an electronic signature system in their management processes and have a digital certificate on a cryptographic card, it might be necessary to provide a cryptographic card reader for teleworking employees.

As a summary of this section: it is important to ensure that all personnel who are going to work remotely have both the minimum resources (PCs and broadband internet connection) and the complementary resources to access and interact with the organiza-

tion's business information systems. Establishing a list and making sure that everyone is properly equipped should be a first step.

- Business Information Systems are accessible from outside the organization

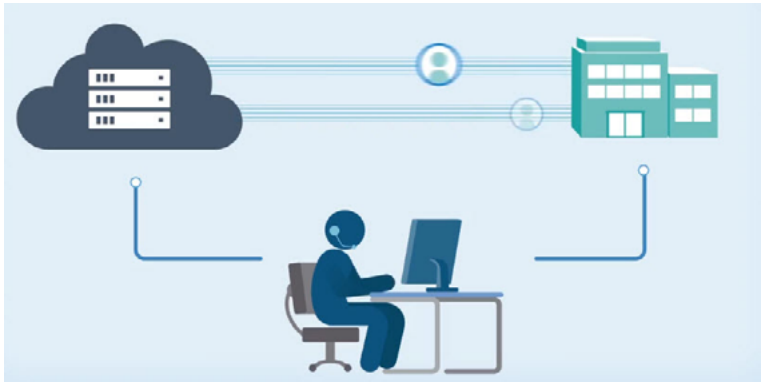
A second step is to make sure that the applications and IT services needed to perform the functions of the employees who are going to telework are accessible from outside the organization and that the user experience is acceptable. The response time of systems and applications must be adequate so that employees are not negatively affected by remote access.

Therefore, it is necessary to provide the means to make corporate systems accessible and usable from outside the organization. To this end, the following points should be considered:

### a) Remote access corporate solution


A remote access solution allows the possibility of establishing what is called a VPN (Virtual Private Network) between remote devices and the organization's network. It creates a secure extension (by establishing an IPSec or SSL tunnel) of the organization's local area network (LAN) over a public and, by default, insecure network such as the internet. There are many manufacturers that offer this type of solution. If it is not available, both alternatives (on-premise or cloud solution) should be assessed to see which one is more suitable for the organization's needs.

*Cloud remote access solution*



If the organization does not yet have a remote access solution installed, it could consider a cloud-based solution, which allows rapid and secure deployment, even if there is limited cloud capacity available within the organization. This type of solution, offered by many manufacturers on a pay-per-use basis, allows temporary access to the organization from any location with the necessary security measures for the type of information handled. It is based on transmitting the presentation layer of the corporate systems to any remote computer as long as the appropriate authentication has been carried out. In this case, it is completely isolated from the corporate network access platform, to prevent putting the corporate systems at risk due to client vulnerabilities.

The architecture needed to provide this type of access falls mainly on the infrastructure used by the cloud. The user only needs to access a web page to authenticate himself/herself and access the corporate services. The only part of the architecture that is the responsibility of each organization is the deployment of a small virtual machine, "Connector", which establishes secure communication between the cloud and the corporate services.

Regardless of the type of remote access solution chosen (on-premise or in the cloud), once implemented, a stress test should be carried out by monitoring the simultaneous connections and analysing the behaviour of the system. A controlled test with the help of the users would be the most reliable and ideal testing method. If this is not possible, the IT department should simulate a load test.

### b) Accessibility to the organization's applications and systems

Web applications and systems that work with standard internet access protocols (e.g. http, https) as well as lightweight user interfaces (e.g. html, JavaScript) should be accessible straight after the VPN connection has been established.

Applications and systems involving heavy user interfaces or non-standard protocols may not offer the required user experience. They may not offer acceptable response times or may not even work. Remote access to this particular type of application should be tested. If they are not efficiently accessible via VPN, a VDI (Virtual Desktop Infrastructure) type solution should be considered.

If the user already has a computer (PC) at their workplace, a quick solution that does not require the implementation of a VDI is for the user to connect remotely by first opening a VPN connection and then an RDP (Remote Desktop Protocol) connection against the office PC. Microsoft Windows has an application/functionality called "Remote Desktop Connection" which allows a connection to be established between Windows computers. This is a quick and simple solution recommended in cases where the remote user is going to connect to a physical corporate computer located in the organization's offices. In this case, certain conditions must be taken into account, such as:

- Depending on the set up chosen, it may be necessary to ensure that some IT equipment located in the port premises (e.g. servers, PC) are kept operational ("turned on") so that the remote access is feasible.
- Enable the WOL (Wake On Lan) functionality so that if necessary (after an involuntary shutdown or power failure) they can be turned on remotely by the IT department.
- The remote computer is a corporate hardened computer that has a security solution for the endpoint.
- The VPN access policy should limit remote users to only establish an RDP connection against their own office equipment.

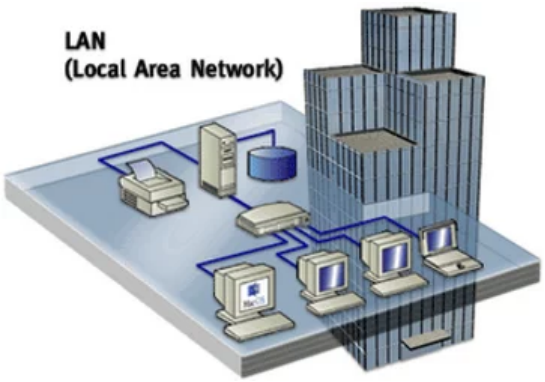
It is not advisable to install any corporate solution or application on personal or non-corporate equipment. Instead, this equipment should only be used as a client to establish a remote RDP connection to the user's perfectly hardened corporate physical equipment or to a virtual desktop (in the case of having a deployed Virtual Desktop Infrastructure).

In cases where it is necessary to install corporate applications on equipment that is not corporately owned, it is recommended to implement an NAC (Network Access Control) type solution that allows the devices to be controlled, guaranteeing that they comply with the organization's security measures prior to establishing the remote connection.

To summarize this section: every remote computer should have a client or VPN access mode, and those who will need access to the remote desktop (either the physical office computer or a virtual desktop) should be provided with an RDP client.

No less important is the fact that a short user manual must be prepared, detailing how to install, connect and disconnect from both the VPN and the Remote Desktop, if applicable. Organizations often tend to focus on the technological means and forget about the users who are going to use them. Therefore, it is important to provide users with clear, simple instructions.

- The communication lines have the necessary and sufficient bandwidth to support remote work




Communication lines—in particular the bandwidth of the internet connection—are designed based on the needs of the organization in a normal situation. In a normal situation, the connection between the corporate information systems and the users is mainly established through the LAN. The capacity of the internet access line is designed so that resources external to the organization (e.g. cloud services, communication with third parties and access to internet services) can access it.

In a pandemic situation, the scenario is reversed. Remote users use their own home WIFI or 4G/5G broadband internet connection to access resources outside the organization (e.g. cloud services, communication with third parties and access to internet services) and consume a corporate internet access line bandwidth when accessing the organization's internal information systems.

It is therefore necessary to make sure that the communication line to the internet is sufficient to support remote work.

As mentioned above, remote access to systems and applications should be agile and should provide a user experience as similar as possible to the one offered in a normal situation. Although light access protocols will always be used after establishing the VPN connection (e.g. http or https for access to web applications and RDP for the rest of the systems and applications), it is necessary to check that the organization's internet connection line is able to support the incoming traffic that working remotely entails.

In order to fulfil this objective, it is recommended to carry out a controlled test by monitoring the bandwidth and taking measurements after opening multiple RDP and VPN connections against the organization's web applications. After these measurements have been made and the number of concurrent RDP and VPN connections estimated, an approximate calculation of the necessary bandwidth can be made.

No less important is the need to provide clear, simple instructions to the members of the organization to prevent the line to the corporate internet from collapsing, by indicating that:

- The VPN connection should only be used to access the organization's internal services, corporate web applications and a remote desktop connection.
- No VPN connection should be established to access cloud services, communicate with third parties or access internet services.

Throughout this section, it has been emphasized that it is important to provide clear, simple instructions on how to proceed for employees who telework. It is recommended that these instructions are accompanied by a small ad-hoc training/webinar. Recording an instructional video and uploading it to the organization's intranet is one option.

## 3.2 Teleworking productivity tools

In a normal situation, the natural proximity of employees and the possibility of travelling to another place or city if required have led organizations to take it for granted that business meetings are held in person.

Therefore, when establishing business relationships (both internally and externally), few organizations have seen the need to implement teleworking solutions (e.g. video-conferencing, chat, working in the cloud, corporate social networks, etc.) because, under the assumption of an on-site presence, the return on investment (ROI) can be low.

In a pandemic situation, the tools that allow colleagues to interact with one another at distance are needed as they eliminate the distance barrier. These tools must be easy to use and must offer a user experience that imitates personal contact as closely as possible.

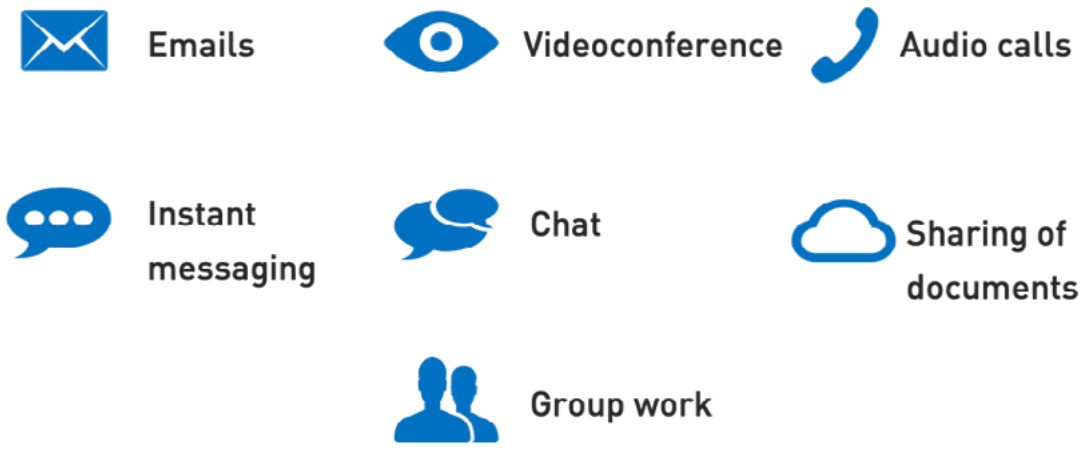
Many tools available on the market can help with teleworking. There are tools specialized in videoconferencing and others that have this functionality but which also incorporate other functions such as individual chat, corporate chat, group work, document sharing and application integration. The latter are called **collaborative platforms**.

In order to be able to deal with a teleworking situation, it is advisable to implement a collaborative solution. Depending on how the chosen solution has developed its videoconferencing capabilities and on the organization's needs in this respect, it may be necessary to complement it with a specialized videoconferencing tool.

In any case, the productivity and videoconferencing tools (if necessary) that are implemented must be multi-device. They must work independently of the device the teleworker has (e.g. smartphone, tablet, laptop, or desktop).

Examples of collaborative platforms are Google Workspace and Microsoft 365, and examples of specialized tools for videoconferencing are Zoom, Microsoft Teams and Cisco Webex.

The **main basic functionalities** that must be provided to remote employees and that are usually offered by these tools are:




- **Email**: Email is the tool par excellence in digital remote communication. Organizations typically already have an email system or service, but they must ensure that this service has been deployed throughout the departments and that every employee has an email account.
- **Videoconference**: A videoconferencing tool replaces face-to-face meetings and should allow agile and efficient interaction between those attending the meetings by providing basic functionalities such as screen sharing and

meeting moderation. It is important to bear in mind that both people from the organization itself and from outside the organization should be able to attend meetings held via videoconference. Therefore, the organization should select a tool that allows participants to be able to join and participate in the virtual meetings independently of the hardware and software installed on their device.

- **Audio calls**: Most of the platforms allow, via the same videoconferencing tool, audio calls to be made to other users of the platform by means of VoIP (voice over internet protocol). Calls to third parties (outside of the platform) and which require connection to the telephone system usually have an additional cost and may require an integration gateway with the corporate telephone system.
- **Instant messaging**: This function allows users to send a "pop-up" message to a specific person, a group of people, or even the entire organization.
- **Chat/channels**: This function allows users to establish specific threads of conversation which can avoid unnecessary and, in some cases, unmanageable emails.
- **Sharing of documents**: This function allows users to store, access and share documents. Some collaborative systems have the capacity of co-authoring which allows users to work on the same file at the same time with automatic and instantaneous synchronization of changes, and also allowing version history to be tracked.
- **Virtual group work spaces**: This function allows users to organize teleworkers by work teams, projects, departments, etc. so that it is easier to interact with a certain predefined group of people (e.g. share documentation, chat, send an instant message, hold a video or audioconference).

Organizations should aim to implement a solution that provides these seven functionalities to facilitate teleworking. Some collaborative platforms can provide additional functions which can complement these basic ones to achieve greater efficiency and agility in collaborative work.

In addition to implementing these software tools, it is important not to overlook the hardware tools needed to run the chosen solution.

The provision of mobile devices such as smartphones or tablets to the management staff is highly recommended since it has been proven that the main user interface used at that level is mobile devices. This would add agility and immediacy to communications.

**Training and online support group**

Finally, no less important than selecting and deploying the necessary tools for teleworking are the planning of training and preparation of teleworkers on their use, and putting in place an online support group to attend to queries or possible incidents.

Depending on the amount of time available to implement the change of work model (from the face-to-face model to the remote one), there will be different **alternatives for training teleworkers**, such as:

- Standard training courses;
- Compressed training session;
- Specific training on most relevant matters; and
- Issuance of technical instructions necessary for urgent implementation.

Since the users will change their work environment and tools, the number of queries and incidents arising from teleworking will almost certainly be high at the beginning. For this reason, it is recommended to put in place an **Online Support Group** for teleworking employees.

- As far as possible, the online support group should be a dedicated and specialized group for this type of incident, and independent from the group dealing with the usual incidents with the organization's systems. The latter must follow the usual route defined by the organization.
- There should be two separate channels: 1) for incidents, and 2) for non-urgent matters such as doubts or queries. This allows the support group to prioritize the problems that prevent employees from starting or continuing teleworking over less urgent doubts or queries about how to use the newly implemented tools.
- Tools that allow remote access and control of the teleworkers' computer by the support team if necessary should be available.
- There should also be solutions available in the event of a problem that cannot be solved remotely. For example, if there is a hardware problem on a teleworker's laptop, a replacement computer can be sent via a messenger service and the problematic one can be picked up to be repaired.

To summarize this section, it is necessary to provide staff with mobility IT equipment as well as collaborative software tools in order to facilitate teleworking. It is also important to train all teleworkers on the use of these resources.

## 3.3 Go paperless

Information flows in a port environment are usually very complex and involve a large number of agents. Each container movement requires multiple communications between the members of the port community, thus creating a complex network of information. This is why a neutral and open electronic system or platform is necessary to allow for an intelligent and secure exchange of information between public and private agents. With this aim in mind, the **Port Community Systems** (PCS) were created.

PCS are aimed at optimizing, managing and automating the port and logistics processes in an efficient way through a single data transmission and connection to the transport and logistics chains, in order to achieve:

- Greater efficiency in transactions;
- Resource optimization;
- Process automation;
- Cost savings;
- Fewer errors;
- Time savings; and
- Better customer service.

In addition to the PCS, the agents or organizations that have opted to digitalize their processes are committing themselves to a paperless culture. There are many reasons for moving towards digital media and encouraging a reduction in the use of paper in the organization. Some of the advantages of a paperless culture are:

- √ **Safety, security and reliability**. Storage in digital format allows us to control all the information, and know who is accessing the documents and when.
- √ **Greater productivity**. Electronic document management speeds up information consultation and management processes.
- √ **Optimization of resources**. Digital storage eliminates the costs of the traditional process derived from, for example, printing, sending items by post and destroying paper.
- √ **Environmental improvement**.
- √ **Electronic signature**. We can sign documents electronically from any location and mobile device, reducing the time needed to close agreements, negotiations, etc.

Fortunately, PCS platforms enable the digitalization of the main processes of the logistics chain. The first step is to determine whether a fully implemented paperless culture already exists. In times of pandemic, where staff are working remotely, processes that are still managed on paper are a handicap. Efforts should be made to digitalize them.

Therefore, it is necessary to identify those processes that are not yet digitalized and tackle them on a case-by-case basis. Depending on the time available to deal with their digitalization, this may be done with a greater or lesser degree of automation.

There are free tools that can help to get rid of paper format processes. The steps to a simple process with little automation could be:

1. **Creation**: Use the text processor (e.g. Microsoft Word or Google Docs) of the collaborative platform to digitalize/convert into standard PDF format (Portable Document Format) any document generated in the organization.
2. **Signature**: If the document requires a signature, the corporate electronic signature holder or the Adobe Acrobat Reader DC application can be used.
3. **Distribution**: Use the email management tools (e.g. Microsoft Outlook or Google Gmail) or document sharing tools (e.g. Microsoft OneDrive/SharePoint or Google Drive) available on the collaborative platform.

These tools and steps should be part of the communication and training phase mentioned in the previous section.

In summary, processes that are still supported in paper format should be identified to help focus digitalization efforts. It is recommended that the transition to paperless be approached gradually. Initially, the maximizing of the automation should not be a priority because of the time needed to do so. That could be addressed at a later stage.

## 3.4 IT security and resilience

In a normal situation, business IT resources are connected and accessible via the organization's LAN. Most applications, databases, equipment (PCs), etc. are interconnected through a reliable and secure network. In this situation, one of the most important pillars of IT security is perimeter security, i.e. a security perimeter is established around the organization's

network. The usual practice is to protect the perimeter of the LAN with firewall type devices, allowing secure access from the computers in the network to the resources outside it and preventing the computers outside from accessing the corporate internal resources and systems.

However, in a teleworking situation, the teleworkers' equipment (e.g. PCs) must leave the secure perimeter established in a normal situation and, for the purposes of the organization's perimeter security system, they will be treated as any other equipment connected to the internet, i.e. as unreliable equipment.

When employees are working remotely it is more difficult to control and stop threats. In this situation, new risks (cyber-risks) arise and must be assessed, dealt with and mitigated to the extent possible.

Below are the recommendations and actions that we must take into account in order to achieve an IT environment that is as secure as possible and, recognizing that it is not possible to guarantee absolute security, to have rapid recovery measures in the event of deliberate attacks. The actions listed include the following:

**General recommendations**

As general protection measures, it is recommended to:

- √ Have the latest operating system updates installed;
- √ Implement a strong authentication protocol and an Active Directory of the organization. In the case of cloud services or VPN access, it is recommended not to have only password access but to have a two-factor authentication (2FA) system;
- √ Protect the BIOS (Basic Input/Output System) with a strong password;
- √ Have specific security solutions in the workstations: complement the traditional and necessary antivirus (EPP - Endpoint Protection Platform) with an EDR (EndPoint Detection and Response) type solution;
- √ Implement a centralized administration policy of work equipment where users do not have administrator credentials;
- √ Protect information. Most professional laptops have a TPM (Trusted Platform Module) chip through which the data on the hard disk can be encrypted, protecting the information even in the event of physical access to the disk;
- √ Have an updated list of people, IP addresses, telephones, emails of personnel who access the systems remotely;
- √ Review records and audit remote connections;
- √ Restrict mounting mapped organization units on unsafe remote computers.

**Diagnose new threats**

Teleworking involves several risks that must be considered beforehand in order to implement the safest solutions.

The start of a crisis such as a pandemic brings with it the need for information. People need to know what to do in the event of contagion, what protective

measures should be taken, how the pandemic is evolving, what provision is made for a vaccine, etc. This fact is taken advantage of by cyber-criminals.

For instance, more than 20,000 domains using COVID-19 related terms have been registered, of which more than 50% of the registrations were made in March 2020 (while in full lockdown in some parts of the world), many of them for clear malicious purposes. Prevention and technology solutions are needed to address these new threats.

**Prevent**


Emails are an entry point for phishing attacks. In a pandemic period, emails with message subjects and addresses that appear to be official and reliable sources addressing the issue of the pandemic abound. However, behind these messages are highly dangerous files or links.

It is important to adequately inform employees of the existence of this danger, as they may be unaware of this reality.

**Train**

The organization should instruct its workers on how to protect their IT equipment and connections when working remotely, and verify that appropriate equipment encryption techniques and secure authentication systems are used. In addition, employees must be trained on how to deal with a threat in line with the organization's protocol for dealing with cyber-attacks. In this respect, it is recommended to carry out a simulated phishing campaign that will help employees understand the problem in a palpable way and train them for real situations.

**Contingency plan**

The best-prepared organizations have a contingency plan that allows them to anticipate the difficulties that may arise. On the contrary, those who have been surprised by the situation without a plan of action and have even been forced to improvise a teleworking system due to the lack of planning, have seen their systems saturated by the increase in remote access traffic and have had to provide remote equipment with security measures against the clock.

No organization wants to stop its activity. To avoid this, a **Business Contingency Plan** must be designed and made available to the workers involved. This plan should be tested periodically to confirm its validity and effectiveness, and updated if necessary. Having an untested or obsolete Contingency Plan is useless.

### Cyber-resilience


Today, organizations are dependent on technology to develop and maintain their activity. In the era of digital transformation, a security breach can bring businesses and production processes to a halt, causing economic losses and other consequences that compromise the continuity of the organization.

**Cyber-resilience** is the ability of an organization to anticipate, resist, recover and evolve to improve its capabilities in the face of adverse conditions, stress or attacks on the cyber-resources it needs to operate.

We say that an organization is cyber-resilient if it is aware that absolute security does not exist and therefore assumes that some attacks will not be stopped. Under the aforementioned premise, it has a plan of action that allows it to resume the organization's activity as soon as possible if such an attack occurs.

The organization that has contingency, continuity and crisis plans in place will be able to overcome a cyber-attack in less time and at a lower economic cost. Planning and prevention are the best ways to ensure proper protection against cyber-attacks and to be able to become a cyber-resilient organization.

### Measuring cyber-resilience

But how cyber-resilient is my organization? What is its level of cyber-resilience? It can only be improved if it can be measured.

There are methods that allow us to measure the degree of cyber-resilience of an organization. The reference framework of cyber-resilience indicators proposed by MITRE[1] is one of the most widespread. This framework is based on the four goals that a cyber-resilient organization must achieve: Anticipate, Resist, Recover and Evolve:

- √ **Anticipate**: maintain a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks.
- √ **Withstand**: continue essential mission/business functions despite successful execution of an attack by an adversary.
- √ **Recover**: restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary.
- √ **Evolve**: change missions/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks.

In order to achieve these four goals and ultimately be considered as a cyber-resilient organization, the following elements should be considered:

1 MITRE (2012), Cyber Resiliency Engineering Framework. www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework

√ **Anticipate**

- Cybersecurity Policy: have a policy that sets out the requirements for cyber-resilience, addresses cyber-security risks, assigns responsibilities and is communicated throughout the organization.
- Risk Management: identify, analyse and mitigate risks to the organization's assets, which could negatively affect the operation and provision of services.
- Cybersecurity Training: promote knowledge and skills development of individuals in support of their roles, to achieve and maintain operational cyber-resilience and protection.

√ **Withstand**

- Vulnerability Management: identify, analyse and manage vulnerabilities in assets that support essential services.
- Ongoing Monitoring: gather, compile and distribute information on the behaviour and activities of systems and people to support the ongoing process of identifying and analysing risks to the organization's assets and essential services that may adversely affect their operation and delivery.

√ **Recover**

- Incident Management: establish processes to identify and analyse events, detect incidents, and determine and implement an appropriate organizational response.
- Service Continuity Management: determine how the organization conducts business planning to ensure the continuity of essential services in the event of an incident or disaster. Special attention is given to the recovery objective, for which there is a backup and restore system (backup or site recovery) that guarantees that there are copies of all the organization's information.

√ **Evolve**

- Management of configuration and of changes: establish processes to maintain the integrity of all assets (technology, information and facilities) required to provide essential services.
- Communication: establish processes to ensure communication between those responsible for the operation of essential services, both internal and external to the organization.

To summarize this section, in a pandemic situation, new risks (cyber-risks) arise that must be assessed, treated and mitigated. To this end, there are a series of recommendations for achieving the safest possible IT environment.

As an organization that is aware that there are risks and threats that cannot be mitigated, it must be able to measure its state of cyber-resilience in order to make progress on those goals that have not yet been achieved and to enable the achievement of the necessary and acceptable degree of cyber-resilience.

The MITRE framework is a good reference framework for measuring the state and improving the degree of cyber-resilience of an organization. This framework is based on four goals (anticipate, resist, recover and evolve), which in turn include a series of functional domains that an organization must work on.