TELEWORKAND INFORMATION SECURITY

PSI-06

The organization,within its headquarters and outside the workplace, it has established that, for the performance of company activities, when appropriate, the following devices owned by the organization and granted for use to staff are used:

- Smartphone
- Tablet
- Laptops

RULES OF USE

The employmentof such devices is governed by the implementing rules:

- The deviceis for personal use
- It cannot be used by anyone other than the assignee
- It must be used for business purposes only, byod (bring your own device, mixed use) is not provided
- Physical maintenance of the deviceis entrusted to the assignee (although supervised by the asset manager)
- Physical protectionof the device is entrusted to the assignee (even if supervised by the asset manager)
- It is forbidden to install software, process files or other utility programs on the device except those provided by the organization or its operation
- It is forbidden to connect hard drives, USB sticks and other memory devices to the device

CONFIGURATIONS FOR SECURITY

Relativelyto configurations, all devices used outside are remotely controlled. It's the same organization which provides, through the system administrator, and in a centralized manner, to:

- Setting up the control of access to the device through authentication
- To install, configure, update and check the antivirus
- To install, configure, update and control the firewall of the single device
- To install, configure, update, and check software and utilities

6.2.1 Teleworking

Contractual provision of teleworking

Our organization providesthat some work activities can be performed outside the premises of its offices and in particular in an environment suitable for:

- To executework effectively and efficiently at least as much as it would be "in the office"
- To guardthe necessary work equipment in a safe manner
- to preservethe security of the information contained in the assets
- Allowthe worker to be able to enjoy "adequate" comfort and the necessary concentration (absence of distractions)

Teleworkingis governed, in accordance with the law and in accordance with the specific regulations on the matter, by the employment contract that binds the organization to the worker, whether this is an individual or collective contract.

Responsibility in teleworking

RDP (Production)has the responsibility:

- Supervision of work activities carried out in the teleworking regime
- The security of the information associated with them
- The preparation of security checks

Telework as a measure for business continuity

The organization considersTelework is an effective tool to be used when sudden and adverse conditions make it impossible to continue working activities within the organization's premises. Teleworking therefore also represents a measure for “business continuity”.

Rulesof prevention for teleworking

The organization,in order to control information security risks in the context of teleworking, it applies the prevention policy based on the following rules:

- Makes personnel aware, through training, of the dangers that can compromise the confidentiality, integrity and availability of information and the security controls to be applied
- Provides portable devices and prohibits the use of personal devices
- Administerteleworking with tools that allow the planning and verification of activities performed remotely
- Provides assistance from the system administrator for solving technical problems
- It makes available assistance from the RGSI for the application of safety procedures
- Prepares specialsoftware utility for reporting the work done remotely
- Prohibits the use of occasional “workstations”

CONTROL OFACCESSES | **PSI-09**

9.1.1 Access control policy

The organization,to protect the confidentiality of information, it has established that only certain people can access the places where they are kept and treated, whether they are physical places (reserved areas, safes, archives, etc.) or logical ones (hard disk, database, etc.).

WHAT'S THISACCESS CONTROL

The accessesto the work areas of the organization and access to the network and network services are controlled so that only those who have been expressly authorized by top management (and controlled by the system administrator) can access the critical information processed in the processes or in any case held for any reason (legitimate) by the organization itself.

THE BUSINESS REQUIREMENTS OF ACCESS CONTROL

Staffwho works in primary (operational) processes must access only the physical areas in which information relating to primary processes is processed and can access, via the computer network, only those network areas (folders / directories) that contain information relating to the processes primary.

The staff employed in the processessupport must access only the physical areas in which support activities are carried out and information belonging to this category of processes is processed.

The staff employed in the processesinformation security, on the other hand, has greater freedom since, due to his duties, he must be able to intervene both physically and electronically in areas where information is handled regardless of the processes to which they belong.

The organization has established that only those who have been expressly authorized can access critical information processed in the processes or in any case held for any reason (legitimate) by the organization itself.

THE APPLICATION OF ACCESS CONTROL IN THE ORGANIZATION

For this necessary limitation, provided for by the access control policy with the aim of protecting information, the organization has identified "access controls" provided for:

- Accessto the company headquarters
- Accessto individual offices (restricted areas)
- Accessthe devices to be used to manage information (computers)
- Accessto the company information system
- Access to paper archives
- Accessto the server room (where the servers are kept)
- Accessto databases that hold security information (e.g. databases of passwords or cryptographic keys)

9.4.3 System password management

The information system of the organization allowsto manage data and information contained within the databaseof the information system itself. In this database, one table is reserved for the registration of **password** that, in any case, they remain encrypted and therefore not understandable.

There password table has been set up to "accept" passwords with the following characteristics:

- Minimum lengthof the 8-character string
- Presenceof lowercase letters (az)
- Presenceof uppercase letters (AZ)
- Presenceof Arabic numerals (0-9)
- Non-alphanumeric characters (for example:?, #, *)

The system predicts the expirationof the password after which the original passwords are no longer active and must be replaced with others that meet the same requirements.

The system provides the user with feedbackregarding the "security" of the chosen password.

The more complex the password, the greater its protective effectiveness in the event of a "brute force" attack. In fact, this attack requires malicious software to formulate many combinations of letters and numbers until it identifies the right one to access.

From this it is also understood why the possible access attempts have been limited to 4. Then the system crashes.

The systempassword management is entrusted to software specifically designed to manage access control to the information system.

This software guarantees:

- Archivingand password management
- Sharing, managementand providing users with passwords
- Remote resetpasswords
- Managementof privileged sessions, remote access and automatic access
- Control, complianceand reports

10.1.2 Managementcryptographic keys

ENCRYPTING FOR E-MAIL COMMUNICATIONSAND RESERVED CHAT

To ensure the confidentiality of email communications that users send and receive between themselves and with the parties interested parties (suppliers, customers, consultants, etc.), all of theme-mails containing level A critical information are submittedchecking the digital signature. Messages and documents are encrypted and authenticated through employment **of this "signature".**

The senderwho communicates through the organization's email, with the application of the digital signature, affixes a “label” to the message ensuring that it was produced by a specific person. The digital signature also allows the organization to guarantee that the message cannot be modified during its journey on the network.

The signaturedigital, which control applied by the organization, as we have already anticipated, is able to guarantee:

- The identity of the sender, providing certainty as to who sent it (authentication)
- Impossibility,for the sender, to deny having sent this message (non repudiation)
- That the message is received exactly as it was sent (integrity)

THE SECURITY MECHANISM AT THE BASIS OF ASYMMETRIC CRYPTOGRAPHY

The organization, as alreadydeclared, employs asymmetric encryption. This typology uses a pair of keys to encrypt and decrypt the data. In practice, the key used by the sender to encrypt the data (an algorithm that makes the information incomprehensible) is different from the key used by the recipient to decrypt it.

The contents that transit the network to reach the recipient, during the journey cannot be intercepted and made understandable to third parties since the decryption key does not travel together with the message sent but is in the possession of only the certain, authentic recipient. The organization through the use of "asymmetric" cryptography ensures the confidentiality of the information and allows that the message received by the recipient cannot be repudiated.

CRYPTOGRAPHY | **PSI-10**

10.1.2 Managementcryptographic keys

The chartthat follows establishes the manner in which to provide for the encryption of critical information from part of the organization.

POLICY OF CRYPTOGRAPHIC CONTROLS OF FILESAND SUPPORTS	
ASSETS TO BE SUBMITTEDCODE	Top management, in relation to the level of criticality of the information to be protected from the risk of loss of confidentiality, establishes which media and which files should be covered by the scan cryptographicin the module MOD-710-M- Asset inventory. The encryptionof the files or media that hold them comes performed by the RGSI (with the help of the system administrator) throughthe software made available by the organization e also indicated in the form MOD-710-M-Inventory of **asset.** **ASSET ENCRYPTION** The assets subjectedencrypted by the organization are: ▪ The hard onesdisk of the server ▪ Data backed up to the cloud ▪ The media in which the configuration data of the network devices ▪ The disks of portable personal computers ▪ Fixed personal computer disks ▪ Theresmartphone memory ▪ Credentialsauthorization for physical access via doors ▪ The fields of the databases ▪ The media in which the configuration data of the devices safety ▪ Software that stores scanned, tracked and copied data for the security of the information system and the network ▪ The audio signals of the telephone communication in internal voip to the organization

11.1.1 Physical security perimeter

The organization protectsinformation on physical hazards that may arise from the outside. In this regard, the organization has defined a physical security perimeter, to protect the information and assets with which it is managed and which are indicated in the MOD-710-M- Asset inventory form.

The controls set up for information security, which constitute the "corporate security perimeter", have been divided by the organization into two types:

Check forphysical security:
who preside over access to the organization by staff, suppliers and other interested parties. Physical security includes those measures that tend to control risks from ill-intentioned people, people whose acts can be targeted:

- Upon accessabusive to information
- To their physical removal (by removing the supports)
- To their destruction

Check forenvironmental safety:
which oversee the protection of assets from threats related to climate, temperature, climatic events.
These threats can involve the partial or total destruction of the assets and information contained within them.

The securityinformation that depends on physical and environmental aspects can be put at risk, eg example, from the following threats:

- Fire
- Explosion
- Blackout
- Flooding
- Overheating

And in these threats we also add those that, even if dependent on people and not on physical or climatic events, jeopardize the "physical security" of assets, such as:

- Physical intrusionof malicious people with the removal or destruction of equipment and systems
- Malicious acts committed by anyone even if not directly related to the organization (vandalism, protests, insurrections, extortion, retaliation)

11.2.5 Transfer of assets

Equipment, informationo software cannot be taken outside the organization's headquarters without prior authorization from top management. As with memory devices (or media), the equipment that leaves the organization for a transfer, in addition to being accompanied by transport documents DDT, must include:

- The compilationof the MOD-710-P Asset Transfer module
- Authorizationby top management
- The enforcement of controlsauthentication for access, encryption and backup
- Transportby means of a qualified carrier (registered in the register of suppliers)
- Supervisionby the RGSI

It is also necessary to affix, on the equipment leaving the organization's headquarters, a non-removable distinctive sign, such as to make it unequivocally identifiable and belonging to the organization (e.g. a hidden label bearing the ID number of the support and the organization logo).

In casetransfer, the RGSI must verify the need to make any assignment records **support for a new manager**, for instance,a new asset manager.

11.2.6Security of equipment and assets outside the premises

On the outsideof the offices of the organization, with the exception of activities carried out in a teleworking regime by people authorized, not other work activities are carried out.

Where the organization intended to arrange the execution of the work activity at external offices (perhaps belonging to third parties or in any case under the control of others) such external offices must have the same requirementssecurity applied for the office governed in this document.

It is appropriate to indicate in this paragraph that the organization has the possibility of accessing an office alternativein the event that a possible disaster would make it impossible to continue the activities operationalin the disaster area.
This hypothesis is governed by the safety procedure PSI-17 - Operational continuity management of the safety of

SAFETYOPERATIONAL | **PSI-12**

12.5.1 Installing the softwareon production systems

Installation, software updateof production, applications and libraries is carried out only by the information system manager who is trained and trained and installs the software after adequate **authorization**of the highdirection.

The information systemand the applications it includes for information management are "produced" within of the organizationby the IT development team which coincides with the marketing department staff and that of the design office. The system development and operation supervisor is responsible for the **informative system**.

The checks provided are as follows:

CHECK	APPLICATION
Only code is present on production systems approved executableand not development code either compilers	In the production area of the information system is present only approved executable codefrom RDP (production)
Applicationsand operating systems are installed only after extensive testingand completed successfully	Tests performed before delivery (steps from designto production) are conducted by the RDP (production)authorizing the passage of the code application.
Tests include usability, security, on the effects on other systems and ease of use and are performed on separate systems (see control 12.1.4)	Codedevelopment and the use of compilers is logically separatefrom that of the production and it is performed on data on the "design" disk and not on the “production” disc. RDP (production) carries out the tests of: ▪ Usability ▪ Safety ▪ Ease of use and if successful, authorizes the transfer code from the design disk to the disk production.
It is ensured that all corresponding schedule are updated	The librariesof the applications of the information system are updated by the system administrator informativeand RDP (production) in relation to needsto use code already developed and tested from the developers. These aspects, from the point of view of the security of the information, are monitored thanks to the module: MOD-710-G- Software evaluation

12.6.1Management of technical vulnerabilities

The technical vulnerabilities of the information system that emerge during its use by users must be:

- Detected
- Described
- Analyze their causes
- Manage with actions

The relative processthe management of the technical vulnerabilities of the information system is governed by the manager **of the information system**.

The identification can take place thanks to the documentationof the vulnerability within the MOD-710-G-Software evaluation module, and in this case the RGSI will report them to the information system manager.

In caseemergency vulnerability is communicated and formalized with the fastest means available to the organization such as: sms, phone calls, e-mails. This communication must consider the risk of unintentionally disseminating information regarding the presence of a technical vulnerability even in the presence of ill-intentioned persons, therefore it must be carried out in an absolutely timely and confidential manner.

If the technical vulnerability is attributable to a "non-conformity" in relation to the provisions of the procedure PROC-1010 - Non-conformities and corrective actions, the information system manager will proceed to describe the detected non-conformity allowing to understand its nature and / or membership class. Subsequently, it will analyze the causes of the technical vulnerability and will manage it by activating the RDPs or the necessary personnel.

These activities conducted by the information system manager are documented in the form: MOD- 1010-A-Non-compliance report, as the organization can recognize these vulnerabilities as a "lack of conformity" with respect to the strategic objective of security global.

12.6.2 Restrictions on Software Installation

The installationof software extraneous to the organization is not allowed to anyone unless authorized by the top direction and under the control of the system administrator and the RGSI.

Such installations, possibly granted for testing and testing, are permitted on computers and networks absolutely separatefrom the network.

COMMUNICATION SECURITY INNET | **PSI-13**

13.1.1 Controlsof network

ThereThe organization's computer network consists of the server, which is the computer that provides the services to the network, the personal computers on which the authorized users use the operating system and its applications. Then there are all the devices that allow the operation of the network in the connections, in the transmission of information packets, in the sorting and distribution of services made available by top management and documented within the MOD-710-M-Inventory of asset

Structureof the organisation's IT network is made up of “assets” (servers, computers, devices). These have been grouped into classes, and each of them is subjected to security checks aimed at averting the risks related to the loss of confidentiality, integrity and availability of information.

The assets of the organization belonging to the “Network**and communications "**it takes a long timein the primary processes that deal with critical information of level A and how much in the secondary processes whose information handled is of level B.

These assets are as follows and function as indicated:

- PROVIDER (Apparatussupply of Internet services)
- CLOUD (Remote Server in which information is duplicated and stored)
- LAN (Local networkinternal to the organization)
- E-MAIL SERVER (Computer providinge-mail services to the organization)
- CENTRAL SERVER (Computer that providesnetwork services to the organization)
- ROUTER (Devicewhich allows you to interface sub-networks which are: Primary, Support and Security)
- SWITCH (Deviceconnection of other devices to the LAN network)
- ACCESS POINT (Devicefor wireless network access)
- CLIENT (Computers inside the organization connectedto the network)
- WIRING (CablesEthernet and optical fiber)
- PHONE

WHAT TO PROTECT

The securityof each asset, as documented in the inventory indicated above, is attributed to an asset manager which oversees and verifies the implementation of the security controls listed in Annex A of the ISO 27001: 2017 Standard regarding:

The computing devices

In computing devices, keeping server and cloud computing services apart, the organization has included:

- Computer
- Smartphones (considered as above)

COMMUNICATION SECURITY INNET | **PSI-13**

13.2.1Policies and procedures for the transfer of information

Transfer outsideof information contained in the files

The data and information present in the company information system are entered and processed:

- By authorized persons within the organization
- By authorized persons with customers, suppliers and other interested parties.

The information system, foras regards the primary processes, it has specific production software that allows to analyze, classify, manage and transform information in a shared work environment in which users perform the activities aimed at obtaining a precise output.

The output can consist of:

- An internal project (functionalto the internal processes of the organization)
- A project for**a customer**(the trueand own service that the organization releases to the customer who commissioned it)

These outputs are not just information present in the form of records in the database of the informative systembut they are real documents (files) in which the procedures and calculations are indicated related to the project (whether internal or external). These “critical” files are the fundamental object of the transfers.

Given the particular criticality of the projects (documents), the organization has established the use of a **softwarefile transfer**which provides for an authentication system by the sender and by the **receiving**.

The transferof the files happens in the following way:

- TheUsers authorized to transfer files authenticate with the transfer software of files
- **Upload files**to be transmitted in a (eg: documents for the customer) "safe box" (virtual memory)
- The software providesto file encryption
- The receiver (e.g. customer or supplier personnel) authenticates with the file transfer software
- The software,upon authentication of the recipient, it decrypts the files and makes them available for download
- The software**track all operations**and its use is monitored by the software responsible for controlling the logs

The software tracksthe operations carried out as part of the transfer activities: sender, recipient, session duration, hours, transferred files, etc.

Information security inherenttheir transfer (both externally and internally) is ensured thanks to the supervised management of these activities.

14.1.1 Analysesand specific information security requirements

The information that the organization intends to protect is managed by the information systemcompany that we can identify in the software platform thanks to which the organization:

- Interacts withcustomers by administering the product / service
- Interacts withsuppliers for the acquisition of products / services
- It carries out the productive activities, throughthe software connected to the platform
- It guardsand makes data relating to the processes available

The company information systemconsists:

- From the database that contains all the information
- From the data access pages
- From the functions (or additional software) that allow you to manage and process data

The functional requirements of the information system

The organization, to performwork activities, determined the functional requirements that the company information system must possess in order to respond to the information and operational needs of the roles that operate in the processes, in the most effective and efficient way possible. They are reconstructed through the sequence of computerized activities that follow the phases of the processes.

The functional requirements of the information system are listed below.

REQUIREMENTSRELATING TO THE CUSTOMER (WHAT THE CUSTOMER MUST BE ABLE TO DO THANKS TO THE
By connecting to the company operating system via the Internet, the customer must be able to:
to) Make the service / product request and establish the requirements
b) Access the contractual conditions governing the service
c) Monitor the production activities related to your requests
d) Making requests, asking questions, raising objections, issuing authorizations
e) Acquire the product / service
f) Take advantage of after-sales assistance
g) Pay for the service
h) Consult with the managers of the organization

ACQUISITION,SYSTEMS DEVELOPMENT AND MAINTENANCE | PSI-14

14.1.2 Security of application services on public networks

The information system of the organizationis a web based system which can be accessed through the Internet. The personnel who work remotely, not present in the organization, sometimes also access applications (programs to work) that are distributed through the operating system platform.

The securityof the application services made available through the Internet is guaranteed by the following measures:

- The application software**is resident on the server**corporateand not present on computers accessing the system
- Of this software, in accordance with the provisions of the relative contracts, the following are determined: intellectual property, licenses for use, fees, modifications and further development
- The software (source code)it is protected by safety devices that have been set up for the protection of critical information such as: access control, encryption, backup, antivirus, etc.
- **The software is documented**and its documentation, adequately protected in the same way as the software, allows to understand its structure, dynamics, functions and services rendered in order to facilitate maintenance interventions.

The organization**it does not use public networks**understandings such as thoseusually made available to users, customers and visitors of hotels, restaurants, railway stations, trains, sports facilities, tourist centers, etc.

14.1.3 Transaction security in application services

COMMUNICATIONSONLINE THROUGH THE INFORMATION SYSTEM

The organization managesinformation thanks to the use of its information system. This system, as more precisely illustrated in the procedure dedicated to the security of its operation, allows information to be processed through the web pages.

Theweb pages are the interfaces through which the user can read, enter and modify information: to collect customer requirements, to write a project and to produce services, authorized users interact with the web pages.

The pagesweb of the company information system make the information present on the information system database visible. The protocol used for communication through web pages is HTTPS (Hyper Text Transfer Protocol Secure). Thanks to this protocol that uses encryption, the information that employees, collaborators or users send cannot be intercepted by an unauthorized third party.

14.2.3 Reviewapplication engineer following the changes

The in fact, the scheme proposed in the previous paragraph constitutes one of the inputs of the management review thanks to which the managers of the RDP processes and those in charge of information security carry out impact assessment (technical review) and formulate the prevention measures to be taken.

Following the impact assessment, the decisions taken regarding prevention strategies to be adopted in correspondence of changes are documentedin the form MOD-930-B- Minutes of the management review.

14.2.4 Limitation to changes in software packages

The softwareto be adopted for the operation of the operating system is basically based on the following technologies:

- Languageprogramming: PHP
- Database: MySQL

Withthe programming language are created the web pages for accessing the data that allow to process the information present in the MySQL database.

Decisions concerningsoftware package changes must document, in the MOD-930-B- module **Minutes of the reviewof direction**:

- The reasons for the absolute need for change
- The consequent disadvantagesto change
- Themeasures to manage the disadvantages resulting from the change

The analysisin this regard, it can be carried out through the scheme reported in the previous paragraphs when illustrating the impact assessment.

The limitationschanges to software packages also generally apply to:

- System software: that relating to the Windows operating system
- Basic software: set of utility programs and procedures
- Application software, for offices, chosen by the organization which is Microsoft Office

MANAGEMENT OF ACCIDENTS RELATED TO INFORMATION SECURITY | **PSI-16**

16.1.1 Liabilityand procedures

Introduction to disaster recoveryorganization plan

In the face of information risks, the organization has already established internal security controls that keep the overall risk at a low level. These controls are documented in the MOD-710-M- Asset inventory. However, the probability that certain accidents may occur, although low, does not make such events impossible.

If the controls applied internally to the structure, aimed at protecting information should result,**in critical, ineffective, compromised, or otherwise non-functional conditions,**the organizationputs in deed of the shares whose purpose is to be able to reacquire, in the shortest possible time, the availability of the **information.**

Scope

The presentprocedure has the purpose of regulating the way in which the organization manages the unexpected unavailability of information caused by the destruction of the media residing in its physical structure (premises, offices and server room).

The causes of the destruction of the supports, as we have seen in the identificationand risk assessment, may consist of physical or atmospheric phenomena such as:

- Flooding
- Earthquakes
- Floods
- Fires

Therethis procedure, which arises from the analysis and assessment of risks, represents the DISASTER **RECOVERY PLAN**which, translated into Italian, should be understood as the Information Retrieval Plan to be implemented in **caseof disaster**.

The organization,in general, for the recovery of information no longer available, it adopts the "backup" whose policy and operation are governed by the safety procedure PSI-12 - Operational safety, in the dedicated paragraph.

The organization adoptsa disaster recovery solution (of which backup is only one component) that was designedin relation to the technical characteristics of the IT structure. Obviously the backup infrastructure is it was carried out compatibly with the organization's funding possibilities.

From a technical point of view, the disaster recovery solution takes into account the amount of information that could be "lost" due to a disastrous event. This quantity is proportional to the time that elapses from the moment of production of a data (for example the creation of a file on the computer by a user) to the moment in which this data is also saved on the disk of the server and the cloud and is in safety thanks to the backup operation.

16.1.1 Liabilityand procedures

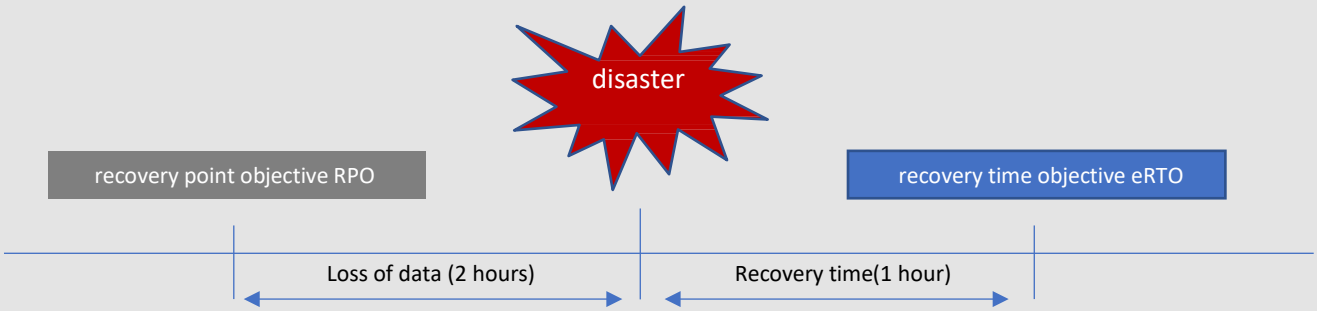
For the "shelter" of information, the organization has opted for a completely redundant IT infrastructure with data replicated off-site. Through the backup, in fact, the information is automatically copied to the provider's "cloud" which, physically, is more than 75 km away from the organization's headquarters. The best practices, in fact, in the field of disaster recovery, suggest a site at least 75 km away in order to displace information that could be lost due to a natural disaster (eg: earthquake).

The organization then calculated the time it would take to restore lost information and reorganize work activities that were interrupted due to an accident.

The organizationestablished the RPO

The Recovery Point Objective (RPO) representsthe maximum time that must elapse between the production of a data and its securing (through backup) and, consequently, offers the measurement of the maximum amount of data that the information system could lose due to sudden failure. This RPO, in the organization, is 2 hours.

If disaster strikes, the organization has all the information (without losing any) that is fully saved every two hours.



The organizationestablished the RTO

The RecoveryTime Objective (RTO) is the recovery time that is required for the total recovery of the operation of the processes. The organizationhas established the RTO at 1 hour. Thanks to the recovery of information lost due to the disaster is theoretically able to leave immediately unless the structure has been compromised ***of the organization.***

OPERATIONAL CONTINUITY MANAGEMENT OF INFORMATION SECURITY | **PSI-17**

17.1.1 Planningthe continuity of information security

This procedure, from a logical and sequential point of view, is connected to the one governing disaster recovery plan, namely the PSI-16 security procedure - Management of incidents relating to information security.

The organization, through suchin fact, the procedure pursues the aim of continuing to operate (and produce) in crisis conditions, ensuring, even in these exceptional circumstances, the security of information from the risks of loss of confidentiality, integrity and availability. The contents of this procedure therefore investigate in greater detail the activities that the organization carries out to "continue working" following the accident that compromised its "operational continuity".

Withthe disaster recovery that the organization has documented within the PSI-16 security procedure - **Management of information security incidents**(often confused withthe continuity of security information), the focus was on retrieving the information and on the actions to be taken to ensure that these become available to users of the operating system.

Attention, in this process focused on business continuity which is different from disaster recovery, yes moves on the restoration of basic activities (production processes towards the customer) and on the functioning of these, in security conditions for information, despite the difficulties due to the temporary impossibility of **operate in optimal conditions.**

To the disaster recovery plan, that is, the one documented through the actions to restore the availability of data, we addthe business continuity plan, that is the planning of the actions that must be carried out by **detection of the "disaster" until recoveryand the management of basic processes**, that is, those that must bein function in order not to interrupt the relationship with the market.

The critical processes for business continuity

If the organization, following a disaster, should find itself in the position of having to continue producing without interruptions (which could compromise the operational continuity of its business), it should have the possibility to:

- **Activate your information system and applications immediately**
- **Giveinformation available again under secure conditions.**

All this is possible in the hypothesis in which, despite the disaster, the personnel of the organization working on the information system can remain at their station. Eg: the organization is undergoing a cyber attack that compromises the integrity of the information present in the information system database.

In this case the organization, having signed a contractfor which its information system and data are stored on a provider's cloud, simply moves the operational activity of users from the information system compromised by the virus and residing on the internal central server, to the "copy" information system residing on the provider cloud.

OPERATIONAL CONTINUITY MANAGEMENT OF INFORMATION SECURITY | **PSI-17**

17.1.3Verification, review and assessment of the continuity of information security

The organizationdesigned the way in which it manages a crisis situation to ensure operational continuity and the relative security of information.

Once a year, the crisis situation is simulated as far as possible in order to verify:

- Immediate availabilityof the alternative site
- Thereability to find the resources necessary for the transfer and activation of the other site
- The response times of the staff
- The actual availability of information
- Effective operationof business processes in an emergency context

The simulation,to lead to realistic results, it is initiated by top management in agreement with the system administrator in a completely realistic manner. The personnel alerted and involved during the exercise, even if aware that it is a simple simulation, must show that they are ready to perform the recovery functions within the agreed time.

The organization, with this simulation of the emergency, carries out the re-examinationactions planned by evaluating its ability to face unexpected events resulting from disasters in time and safely.

This review is similar to that indicated in the procedure relating to hospitalization and the restoration of the availability of PSI-16 information- **Management of information security incidents.**

Thethe results of the simulation of a transfer to the emergency site are subject to management review only once a year. On that occasion, they must be documented among the management review inputs in correspondence with and concurrently with the inputs regarding the evidence relating to security incidents.

17.2.1 Availability of information processing facilities

Thereredundancy of data processing facilities is ensured to the extent that allows to the organizationto continue to operate with reference only to the processes considered critical, that is, those that, during the crisis, keep relationships with customers and suppliers alive.

Availabilityof computers and devices is, in part, ensured by their redundant presence within the same operational structure of the organization. It it is also ensured by the service contract that the organizationhas signed up to take advantage of the alternative site and the resources contained within it.

18.1.1 Identificationapplicable legislation and contractual requirements

The protectionof the information, which is the strategic objective of the organization pursued through this management system, must be designed, conceived and implemented in relation to the requirements of the ISO 27001 standard and the controls established by it.

This compliance is explained, respectively, within the management procedures and within the safety procedures. However, there are other requirements that the organization must comply with in its information protection activity which are:

- **The contractual requirements**
  That the organization collects and reviews as governed by the procedure PROC-812- Requirements. These requirements are expressed by the customer and concern the level of information security expected by the customer. The customer expresses the "security for his information" requirements that must be elaborated by the organization with reference to specific level service agreements. The entire safety apparatus of the organization has been conceived to cover the safety needs of the clients.

- **The requirements provided for by current legislation**
  Which are requirements imposed by laws that pursue purposes that, in some way, are connected or in any case can be influenced by the way in which the organization protects information. The relevant legislation is as follows:

  - The rulesEuropean Commission on the protection of individuals with reference to personal data n. 679/2016 (GDPR)
  - The Measureof the Guarantor: Measures and precautions prescribed to the owners of the treatments carried out with electronic tools in relation to the attributions of the functions of system administrator
    n. November 27, 2008
  - Art. 2.8 of the lawon copyright (Law 633/41), with reference to the intellectual property of software

Behaviorof the people who process the information within the organization, in addition to being determined by the procedures governing security controls is also regulated by law. Attacks on information security, in addition to being averted by controls and prevention measures, are also foreseen and punished by the criminal code.

L'article 615-ter of the criminal code provides for unauthorized access to a computer system against consent explicit or implicit of the person having the right to exclude third parties from obtaining such access. The penalty is there imprisonment for up to 3 years.

18.1.2 Intellectual Property Rights

Rights organization considerationsowned by the software

The Italian legal system,following the transposition of European standards such as Directive 2009/24 / EC, admits the protection of computer programs through Art. 2 paragraph 8 of the copyright law (L. 633/41) **updated**,which establishes that “computer programs, in any form expressed as long as they are original as a result of the author's intellectual creation. The term "program" comprehendsalso the preparatory material for the design of the program itself.

Copyright (rightof copy) allows its owner to control the use aimed at the economic exploitation of an intellectual work, in this case of the computer program. This possibility derives from the recognition of the exclusive property rights of the software, pursuant to Article 64-bis of the law on the protection of copyright, whose legislation is configured as a specification of the general rules on economic rights established in general all intellectual property from Articles 12-19 of the law on the protection of copyright.

Organization choices

The organization providesto regulate any objects of the dispute, indicated in the previous table, through contracts which, in accordance with the provisions of the law on the protection of copyright L. 633/1941, regulate the production of systems and software that is exchanged between the organization And:

- Employees (employment contract)
- Suppliers / consultants (supply contract and framework agreements)
- Customers (contract and order specifications)

The organization,for the purpose of an easy resolution of the dispute, it has established that the software that any contenders want to claim, must be filed with the Special Public Register for Computer Programs or filed as an unpublished work if the software itself has not yet been published or used .

Patent appeal

If the organization considers that its "own" software has the special requirements (creativity, originality) provided for by the legislation relating to "inventions", it will patent the software by checking:

- Theright of economic exploitation of the software
- Theright to carry out or authorize:
  - Reproduction, translation, adaptation, transformation, modification
  - Distribution in any form