apdcat
Autoritat Catalana de Protecció de Dades

DPIA Template

A Data Protection Impact Assessment (DPIA) is a procedure that seeks to identify and control the risks to the rights and freedoms of the people that result from personal data processing.

A description of the processing is needed to determine if a DPIA is needed. This description should have a level of detail enough to allow us to evaluate the risk indicators given below.

Description of the processing

In the following cases, there is no need to conduct a DPIA:

Case	
The processing has nature, scope, context, and purpose similar to another processing for which a DPIA has already been done.	
The processing has a legal basis in the law of the EU or a Member State, and an AIPD has already been performed at the time of adopting such a legal basis..	

Justification

When none of the previous cases apply, a DPIA must be conducted if the processing is likely to result in a high risk to the rights and freedoms of natural persons. The Article 29 Working Party (WP29) gives the following list of characteristics that can be indicative of a high risk.

Indicators of high risk	
Evaluation or scoring, including profiling and predicting.	
Automated-decision making with legal or other significant effect.	
Systematic monitoring.	

Indicators of high risk	
Systematic monitoring.	
Data processed on a large scale.	
Data sets that have been matched or combined.	
Data concerning vulnerable data subjects.	
Innovative use or applying new technological or organizational solutions.	
Processing that prevents data subjects from exercising a right or using a service or a contract.	

According to the WP29, we need to conduct a DPIA when the processing has two or more of the previous characteristics. Although, the WP29 remarks that a DPIA can be convenient in some cases, even if only one of the previous characteristics applies. If two or more of the previous characteristics apply and we consider that there is no need to conduct a DPIA, we need to justify it.

Must a DPIA be conducted? Why?

We must take into account the opinion of the DPO ragarding the need to conduct a DPIA.

Opinion of the DPO

1. Description of the processing

A detailed description of the processing should be made, as this will be the basis for assessing the need, proportionality, and risks of the processing.

Detailed description of the processing

Purpose of the processing

1.1 Personal data

Data properties are relevant when determining the risks of the processing and to comply with some of the provisions in the regulation.

Data type	
Source	
Conservation period	
Especially sensitive data?	
Purpose different from the collection purpose?	

Data type	
Source	
Conservation period	
Especially sensitive data?	
Purpose different from the collection purpose?	

1.2 Parties involved in the processing

The parties that participate in the data processing, their function, and the data that they process are important factors when determining the risk of the processing.

Party	
Processing operation	
Description	

Party	
Processing operation	
Description	

1.3 Processing operations

This section aims at splitting the processing into smaller parts that are more coherent and easier to deal with.

Processing operation	
Description	
Data	
Outcome	
Recipient	
Place	

Processing operation	
Description	
Data	
Outcome	
Recipient	
Place	

1.4 Data transfers

Sharing data with third parties can increase the risk of the processing; particularly when such sharing involves data transfers to third countries or international organizations where the GDPR does not apply.

Which data is being shared? Tell de recipient and the purpose

2. Necessity and Proportionality

The necessity and proportionality of the processing are evaluated in relation to the purpose of the treatment, which was described in the previous section.

2.1 Purpose of the processing

In principle, the data collected is used to achieve the purpose of the treatment that motivated the collection. However, in some cases, the Regulation allows the processing of data that has been collected for a different purpose.

Are data collected for a purpose other than the purpose of this processing used?	☐ Yes ☐ No

If yes

The following conditions allow the processing of the data for a purpose other than that of the collection.	
Data subjects have consented to the usage of their data for the new purpose.	
The processing is based on the law of the Union or of the Member States that constitutes a measure to safeguard.	
National security	
Defense	
Public safety	
The prevention, investigation, detection, and prosecution of criminal offenses.	
Other important goals of public interest.	
The protection of judicial independence and of judicial procedures.	

If yes

The prevention, investigation, detection, and prosecution of violations of ethical standards.	
The protection of the interested party or the rights and freedoms of others.	
The execution of civil lawsuits.	

If none of the previous conditions apply, the new purpose must be compatible with the purpose that motivated the collection of the data.

Initial purpose	
Data	
New purpose	
Justification of compatibility	

If none of the previous conditions apply, the new purpose must be compatible with the purpose that motivated the collection of the data.

Initial purpose	
Data	
New purpose	
Justification of compatibility	

2.2 Lawfulness and fairness principles

2.2.1 Legal base

For a processing to be lawful, one of the following legal base must apply:

The data subject has given consent to the processing of his or her personal data for one or more specific purposes.	
Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.	
Processing is necessary for compliance with a legal obligation to which the controller is subject.	
Processing is necessary in order to protect the vital interests of the data subject or of another natural person.	
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	
Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	

Justification of the lawfulness

Apart from having a legal base, the processing must not be illicit in wider sense. For instance, it must not infringe copyright or contractual agreements.

Confirm that the processing does not incur in any illicit

2.2.2 Child data processing

Children need special protection with respect to the processing of their data, because they may not be aware of the risks involved.

Is the processing is related to the direct provision of services of the information society to children and has consent as its legal basis?	☐ Yes ☐ No
If yes, has the minimum age for valid consent taken into account?	☐ Yes ☐ No

2.2.3 Processing special categories

Are special categories of data processed?	☐ Yes ☐ No

If yes

We need to determine one of the conditions of article 9 that allows the processing.	
The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where a Union or Member State law prohibits it.	
Processing is necessary for the purposes of carrying out the obligations in the field of employment, social security, and social protection law.	
The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.	
Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.	
Processing relates to personal data which are manifestly made public by the data subject.	
Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.	
Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health.	
Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.	
Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.	

Justification

2.2.4 Processing data related to criminal convictions and offenses

Are data on convictions or criminal offenses processed?	☐ Yes ☐ No

If yes

Although not a special category of data, the data on convictions or criminal offenses also enjoy special protection. The processing of these data is only allowed under the supervision of the public authorities or when authorized by the right of the union or the member state. In addition, when the processing involves comprehensive records of criminal convictions, these must be kept under the control of the authority.

Justification

2.2.5 Validity of consent

For consent to be valid the following conditions must be met:

The controller must be able to show that consent has been collected.	
The request for consent must be intelligible, easily accessible and use a clear language.	
The execution of a contract cannot be subject to receiving consent to process personal data that are not necessary to execute the contract.	
The data subjects have been informed of the possibility of withdrawing their consent at any time.	

2.2.6 Data transfers

To prevent data subjects from having their rights diminished, the GDPR is particularly restrictive with data transfers to countries or international organizations where the GDPR does not apply.

Are data transferred to countries or international organizations where the GDPR does not apply?	☐ Yes ☐ No

If yes

Such transfers are allowed if the European Commission considers that the country or international organization offers an appropriate level of protection, if sufficient guarantees (following article 46) have been established, or if any of the exceptions in article 46 apply

Transferred data	
Destination	
Condition that enables the transfer	

Transferred data	
Destination	
Condition that enables the transfer	

2.2.7 Fairness of the processing

Processing is fair if the use of data it makes (in relation to the purpose of the processing) can be anticipated by the data subjects and does not result in adverse consequences for the data subjects that are not justifiable.

Justification of the fairness

2.3 Minimization principle

Data must be adequate (sufficient to comply with the purpose of the processing), relevant (related to the purpose of the processing) and limited to what is strictly necessary to fulfill the purpose of the processing.

Data type	

Justification of adequacy, relevancy and necessity

Data type	

Justification of adequacy, relevancy and necessity

2.4 Storage limitation principle

Personal data should only be kept for as long as it is necessary to meet the purpose of the processing.

In the description of the processing, we specified the storage period. We need to justify that those periods comply with the storage limitation principle.

Justification of compliance with the storage limitation principle

Mechanisms to delete data that is no longer necessary must be established and made effective. Topics such as the initiation procedure (automatic or manual), the data present in backup copies (how long do they remain there and how do we guarantee that they are not processed?), etc.

Describe the mechanisms to delete data

Data can be kept indefinitely for the purpose of archiving in the public interest, for the purpose of scientific or historical research, or for statistical purposes.

Are data kept for the purpose of archiving in the public interest, for the purpose of scientific or historical research, or for statistical purposes?	

If yes, describe the measures established to guarantee the minimization principle

2.5 Accuracy principle

The processing of inaccurate data can have a negative impact on data subjects. The accuracy principle requires data to be accurate and demands the controller to establish appropriate measures to ensure any inaccuracy is amended without delay.

Controls to guarantee data quality

Measures to correct inaccurate data

2.6 Risks for the data subjects

The goal is to identify any potential negative effects of the processing on the data subjects, quantify risk associated them and, if needed, propose measures to reduce the risk.

In this section, we evaluate the risk associated to the processing in itself. That is, we do not consider the risks associated to security breaches (be it accidental or intentional).

Potential negative effects are very dependent on the actual processing. To help us identify all relevant negative effects, it is convenient to gather the opinion of the data subjects and the data protection officer.

Potential negative effects of the processing

For each of the potential negative effects identified, we estimate the associated risk. The risk depends on two factors: the impact it has on people (low, medium, high or very high) and the probability that it will materialize (low, medium, high). The impact is estimated directly from the potential effects. In order to determine the probability, it is necessary to analyze the circumstances that materialize the negative effects (the threats) and to estimate their probability.

Risk is determined based on the estimated probability and impact, using the following table:

	Impact			
Probability	Low	Medium	High	Very high
High	Medium risk	High risk	High risk	High risk
Medium	Low risk	Medium risk	High risk	High risk
Low	Low risk	Low risk	Medium risk	High risk

Effect on data subjects:

Impact:

Threat	Probability	Risk

Estimated Risk

Effect on data subjects:

Impact:

Effect on data subjects:

Threat	Probability	Risk

Estimated Risk

Unless the risk is low, measures must be taken to reduce it. This is especially necessary for high or very high risks. If it is not possible to reduce a high risk, we must consult the competent data protection authority about the suitability of the processing before we start it.

If the processing has been altered to make it less harmful to the people, the previous sections of the DPIA need to be revised and updated.

2.7 Necessity and proportionality

Using the information gathered in this section, we need to justify that the processing is necessary (the purpose cannot be met by less intrusive means) and proportional (benefits exceed harms).

Justification of the effectiveness of the processing

Justification of the necessity of the processing

Justification of the proportionality of the processing

2.8 Opinion of the data subjects

The GDPR establishes that we should seek the opinion of the data subjects.

Opinion of the data subjects about the necessity and proportionality of the processing

If the controller deems gathering data subjects' opinion inappropriate, it must justify it.

Why hasn't data subjects' opinion been collected?

If the opinion of the data subjects differs from the vision of the controller (section 2.7) and the controller plans to go ahead with the processing, the controller must justify the reason why.

Why is the processing conducted despite the discrepancies of the data subjects?

3. Controls to Guarantee the Rights of Data Subjects

3.1 Transparency controls

Transparency is transversal and must be present in all communications with data subjects.

All communication with data subjects must be concise, intelligible, easily accessible and make use of clear and simple language.	☐ Yes ☐ No

The GDPR specifies how this communication must be done.

The information will be given in writing (including electronic media).	☐ Yes ☐ No
In the case of requests made by electronic means, the information will preferably be given electronically.	☐ Yes ☐ No
If requested, the information will be given orally.	☐ Yes ☐ No

The controller must respond to requests for the exercise of the rights of data subjects within the established deadlines:

Without undue delay and not later than a month.	☐ Yes ☐ No
If the complexity or the number of requests justifies it, the period may be extended to two months. In this case, the reasons must be reported within the first month.	☐ Yes ☐ No

If the controller does not plan to process a request for the exercise of the rights of a data subject, it is necessary to:

Notify the interested party of this fact without undue delay and not later than a month.	☐ Yes ☐ No
Explain the reasons why the request was not fulfilled (for example, the request is repetitive or the person in charge cannot identify the data subject).	☐ Yes ☐ No
Inform about the possibility of appealing the decision to a supervisory authority or a court.	☐ Yes ☐ No

Only if the request is excessive (for example, repetitive) can a fee be charged to cover the costs of processing it.	☐ Yes ☐ No

3.2 Right to be informed

Data subjects have the right to be informed about the collection and subsequent processing of their data.

Articles 13 and 14 specify that data subjects must be informed about the following topics:

The identity and contact details of the controller	☐ Yes ☐ No
Contact data of the data protection officer (if any)	☐ Yes ☐ No
The purpose of the processing	☐ Yes ☐ No
The legal basis of the processing	☐ Yes ☐ No
The legitimate interest of the controller, if this is the legal basis of the processing	☐ Yes ☐ No
The recipients or categories of recipients of the data	☐ Yes ☐ No
The period of retention of the data or the criterion used to determine it	☐ Yes ☐ No
The intention to transfer the data outside the EU, if applicable	☐ Yes ☐ No
The decision of the European Commission regarding the sufficiency of the security offered by the recipient country or organization	☐ Yes ☐ No
The existence of the right to access the data	☐ Yes ☐ No
The existence of right to rectify and suppress	☐ Yes ☐ No
The existence of right to limit the processing	☐ Yes ☐ No
The existence of right to object to the processing	☐ Yes ☐ No
The existence of right to data portability	☐ Yes ☐ No
The existence of right to revoke consent (if this is the legal basis of the processing)	☐ Yes ☐ No
The existence of right to file a complaint with a supervisory authority	☐ Yes ☐ No
That the communication of the data is a legal or contractual requirement, if that is the case	☐ Yes ☐ No
The existence of automated decisions, if that is the case	☐ Yes ☐ No
The intention to process the data for a purpose other than the one that motivated data collection, if that is the case	☐ Yes ☐ No
The origin of the data, if they were not collected directly from data subjects	☐ Yes ☐ No

There are some exemptions to the obligation to inform, which depend on how the data has been collected:

- if the data were obtained directly from the data subject, there is no obligation to inform you if you already have the information;
- if the data were not obtained directly from the data subject, there is no obligation to inform you if one of the following conditions applies: the data subject already has this information, the communication is impossible or requires a disproportionate effort, it is regulated by an EU or member state rules, or the information is confidential on the basis of professional secrecy.

If the data subject is not informed, it is necessary to justify it.

Does the right to be informed applies to all the data?	
If there is some exception, tell which one, to which data, and why	

If information to the data subjects is provided, the GDPR specifies when it must be provided[1].

When data are collected directly from data subjects, the previous information must be provided at the time of data collection.	☐ Yes ☐ No
When data is not collected directly from the interested parties, it is necessary to inform	
Within a reasonable period after obtaining the personal data, but at the latest within one month.	☐ Yes ☐ No
If the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject.	☐ Yes ☐ No
If a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.	☐ Yes ☐ No

3.3 Right to access

Data subjects have the right to obtain from the controller the confirmation that their data are being processed and, in that case, the right to access the personal data and the following information:

[1] GDPR art 13(1) y 14(3),

The purpose of the processing	☐ Yes ☐ No
The data categories processed	☐ Yes ☐ No
The recipients of the data	☐ Yes ☐ No
The retention period of the data	☐ Yes ☐ No
The right to rectify and to erase the data	☐ Yes ☐ No
The right to restrict and to oppose to the processing	☐ Yes ☐ No
The right to lodge a complaint with a supervisory authority	☐ Yes ☐ No
The source of the data, if they were not collected from the data subject	☐ Yes ☐ No
The existence of automated decisions, if it is the case	☐ Yes ☐ No
The guarantees on the transfer of data outside the EU, where appropriate	☐ Yes ☐ No

The controller must make sure that appropriate mechanisms are established for data subjects to exercise the right to access.

Is there a standard procedure to manage right-to-access requests?	☐ Yes ☐ No
Are the personnel that deal with data subjects capacitated to recognize right-to-access requests?	☐ Yes ☐ No

3.4 Right to rectification

Data subjects have the right to rectify personal information that is not accurate.

Is there a standard procedure to manage right-to-rectification requests?	☐ Yes ☐ No
Are the personnel that deal with data subjects capacitated to recognize right-to-rectification requests?	☐ Yes ☐ No

If the controller has shared the data, appropriate steps must be taken to inform recipients about the request for rectification (considering the costs and technology available).

Is there a procedure to notify data recipients about rectifications?	☐ Yes ☐ No

3.5 Right to erasure

A data subject has the right to have data erased in the following cases:

- Data are no longer necessary in relation to the purpose for which they were collected.
- The data subject withdraws their consent and there is no other legal basis for the processing.
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing.
- The data have been processed unlawfully.
- The data must be erased in accordance with a legal obligation to which the controller is subject.
- The data is used to offer information society services to children.

The right to erasure does not apply when the processing is necessary:

- For exercising the right of freedom of expression and information.
- For compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For reasons of public interest in the area of public health.
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, if compliance with these purposes is affected by the erasure of the data.
- For the establishment, exercise or defense of legal claims.

Are the personnel capacitated to determine if the right to erasure applies?	☐ Yes ☐ No

It is advisable to establish a standard channel so that interested parties can ask for the right to erasure. However, the personnel must be able to detect requests made by other means.

Is there a standard procedure to manage right-to-erasure requests?	☐ Yes ☐ No
Are the personnel that deal with data subjects capacitated to recognize right-to-erasure requests?	☐ Yes ☐ No

If the controller has shared the data, appropriate steps must be taken to inform recipients about the right-to-erasure request (considering the costs and technology available).

Is there a procedure to notify data recipients about right-to-erasure request?	☐ Yes ☐ No

3.6 Right to limit processing

Data subjects have the right to limit the processing of their data, in the following cases:

- The data subject has requested the rectification of data and the controller is checking their accuracy.
- The processing is unlawful.
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.
- The data subject has objected to processing but the controller is checking whether the legitimate grounds of the controller override those of the data subject.

Are the personnel capacitated to determine if the right to limit processing applies?	☐ Yes ☐ No

It is advisable to establish a standard channel so that interested parties can ask for the right to limit processing. However, the personnel must be able to detect requests made by other means.

Is there a standard procedure to manage right-to-limit-processing requests?	☐ Yes ☐ No
Are the personnel that deal with data subjects capacitated to recognize right-to-limit-processing requests?	☐ Yes ☐ No

When limiting the processing, we must consider the different forms of processing: collection, analysis, dissemination, etc.

Have all different forms of processing been considered when limiting processing?	☐ Yes ☐ No

If the controller has shared the data, appropriate steps must be taken to inform recipients about the right-to-limit-processing request (considering the costs and technology available).

Is there a procedure to notify data recipients about right-to-limit-processing request?	☐ Yes ☐ No

3.7 Right to data portability

Data subjects have the right to request the data they have provided to the controller in the following cases:

- If the processing is based on the consent or is necessary to execute a contract or to apply pre-contractual measures.
- The processing is done through automated means.

The right to data portability is not limited to the data that data subjects have explicitly given; it also affects the data collected from the observation of data subjects.

Are the personnel capacitated to determine if the right to data portability applies?	☐ Yes ☐ No

The right to data portability should not adversely affect other people. In particular:

- If the personal data contain information related to a third person, it is necessary to evaluate if the rights and freedoms of the latter may be affected.
- If the data relate to several people (for example, a shared bank account), we must seek the consensus of all those interested.

Does the procedure to make the right to data portability effective take into account potential adverse effects on other data subjects?	☐ Yes ☐ No

It is advisable to establish a standard channel so that interested parties can ask for the right to data portability. However, the personnel must be able to detect requests made by other means.

Is there a standard procedure to manage right-to-data-portability requests?	☐ Yes ☐ No
Are the personnel that deal with data subjects capacitated to recognize right-to-data-portability requests?	☐ Yes ☐ No

The GDPR determines the form of the portability.

Is an easy-readable common structured format used?	☐ Yes ☐ No

3.8 Right to object

Data subjects have the right to object to the processing of their data when the processing is based on:

- Public interest or the exercise of public powers conferred on the person in charge of the treatment.
- The legitimate interest of the controller. In this case, the controller must stop the processing, unless the legitimate reasons prevail over the rights of the data subject.

Are the personnel capacitated to determine if the right to object applies?	☐ Yes ☐ No

It is advisable to establish a standard channel so that interested parties can ask for the right to data portability. However, the personnel must be able to detect requests made by other means.

Is there a standard procedure to manage right-to-object requests?	☐ Yes ☐ No
Are the personnel that deal with data subjects capacitated to recognize right-to-object requests?	☐ Yes ☐ No

In some cases, the GDPR specifies how to proceed when receiving a right-to-object requests.

Opposition to processing for marketing purposes. In this case, the controller must stop the processing without exception.	☐ Yes ☐ No
Opposition to processing for scientific or historical research, or for statistical purposes. In this case, the controller may continue the processing if it is justified by the public interest.	☐ Yes ☐ No

3.9 Right not to be subject to automatic decisions

Does the processing have legal effects or have another significant effect on data subjects?	☐ Yes ☐ No
If yes, the processing is only allowed in the following cases	
It is necessary for entering into, or performance of, a contract between the data subject and a data controller	
It is authorized by a UE or a member state law	
It is based on the explicit consent of the data subject	

The data subject has the right to obtain human intervention, to express her or his point of view, and to challenge the decision.

Is there a procedure for data subjects to ask for human intervention, to express her or his point of view, and to challenge the decision?	☐ Yes ☐ No
Do the personnel have the capacity to review and change automated decisions?	☐ Yes ☐ No

Automated decisions can only make use of special categories of data if the data subject has given explicit consent, or if the processing is done to protect the vital interests of the data subject or another person.

Does the automatic decision depend on special categories of data?	☐ Yes ☐ No
If yes, the processing is only allowed in the following cases	
The data subject has given explicit consent	
The processing is done to protect the vital interests of the data subject or another person	

4. Information Security Risks

According to the GDPR, the level of security must be adequate to the risk to the rights and freedoms of data subjects. In this section, we evaluate the risk from the point of view of information security; that is, the risk associated to a breach in the confidentiality, integrity or availability of the data.

4.1 Impact

We evaluate the impact that a loss of confidentiality, integrity and availability has on data subjects.

To determine the impact level, it is necessary to consider the characteristics of the processing. The following situations increase the risk:

- Processing of special categories or other particularly sensitive data (financial information, locations, etc.).
- Monitoring of people.
- Processing data related to groups with special needs (children, authorities, etc.).
- The processing of large amounts of data of each data subject.

To determine the impact, we should consider all possible situations that lead to a loss of confidentiality, integrity, and availability. To facilitate this task, we list some scenarios in which some of these properties are lost.

Impact of a confidentiality breach (that is, of an unauthorized access to the data). Examples involving a breach in data confidentiality:

- The loss or theft of a computer that contains personal data.
- To send by mistake an email containing personal data to an unauthorized person.
- Unauthorized access to a person's account.
- Configuration error in a web that exposes the personal data of its users.
- To steal information from the facilities of the controller.
- An employee access customers' information for illegitimate purposes.

Impact

Low	Medium	High	Very high

Justification

Impact of an integrity breach (that is, of an unauthorized modification of the data)
Examples that involve an integrity breach:

- An employee modifies the data of a client by mistake.
- An error in the communications network alters the data while in transit.
- A company maintains several copies of the data, but a change in one of the copies does not propagate to the others.
- Some information is lost due to a failure in one of the IT systems.

Impact

Low	Medium	High	Very high

Justification

Impact of a loss of availability.
Examples that involve a loss of availability:

- A file is corrupted or deleted and there is no backup.
- A paper document is lost, and there are no copies of it.
- A data access service is not available.

Impact

Low	Medium	High	Very high

Justification

The impact over the processing system is the maximum of the previous impacts.

Impact			
Low	Medium	High	Very high

Justification

4.2 Initial probability

We estimate the probability based on some characteristics of the system that make it more prone to suffer from attacks.

Hardware and software

Q1. Is the processing system connected to external systems? The connection with external systems increases exposure to threats. For example, information may be captured or maliciously modified while in transit, security breaches in the external system may put the security of the data at risk, etc. Examples: ▪ The processing system of a hospital is connected to the systems of several private insurance companies. A security breach in the systems of the insurance companies may put the data processed by the hospital at risk. ▪ Workstations that are part of the processing system have access to the Internet.	☐ Yes ☐ No

Hardware and software

Q2. Is any part of the processing done through the internet? Interaction with data subjects through the Internet exposes the processing system to external threats, such as phishing, SQL injection, man-in-the-middle attacks, DoS and XSS. These threats may compromise the processing system and the security of the data (confidentiality, integrity, and availability). Allowing the personnel of the organization to access the processing system over the Internet increases exposure to external attacks and, also, increases the probability of workers misusing the information (accidentally or intentionally). Examples: ▪ Online stores, online banking, etc. ▪ The use of e-mail as part of the processing system introduces several threats. First, many times, e-mails are not encrypted, which may put the confidentiality of the data at risk. Additionally, the use of e-mail increases the probability of suffering e-mail phishing and spoofing attacks. ▪ The administrators of the processing system can do maintenance tasks over the internet. ▪ The access to the processing system from a public place (e.g. public transportation, bar, etc.) may put the confidentiality of the data at risk	☐ Yes ☐ No
Q3. Is there a failure to follow a relevant good practices document in the design and the configuration of the processing system? If the processing system is not well designed or the elements that compose it are not properly configured, data security risks increase. There are many good-practices guides dealing with different security-related topics (networks, computers, etc.). Examples: ▪ The design of the network must follow a good-practices document that includes elements such as firewalls, network segmentation, and VPN usage. ▪ The configuration of the computers used must follow a good practices document. The number of aspects that need to be considered when configuring a computer is so large that following a document is essential. For instance, user privileges, antivirus, strong passwords, system lock after an inactivity periods are just a few topics. ▪ The processing system should be sized considering the computing, communication and storage needs that are anticipated. Additionally, it must be provided with enough staff. ▪ The configuration of the software used must follow a good-practices document. For example, securing a web server, etc. ▪ The development methodology must take the security of the data into account throughout the entire life cycle of the application.	☐ Yes ☐ No

Hardware and software

Q4. Is there a lack of following a relevant good practices document in the maintenance, monitorization and response to incidents? It is essential to maintain and monitor the system properly. Maintenance must be made both for devices and software. Monitoring the system allows incidents to be analyzed once they have happened. Monitoring may also be used to detect suspicious behavior to prevent security incidents from happening, and to improve the reaction time, thus, reducing their impact. Examples: ▪ Failure to apply operating system security updates can lead to new attack vectors. ▪ The lack of regular backups can lead to the loss of information in case of an incident.	☐ Yes ☐ No
Q5. Is there a lack of physical security in the processing facilities? The physical security of the processing facilities is essential. Without it, the security of the processing system (electronic or not) cannot be guaranteed. Examples: ▪ If the data center lacks appropriate access controls, we cannot prevent unauthorized people from entering it. ▪ Due to space limitations of the physical archiving facilities, documents are being kept in other places that do not offer the necessary security guarantees. ▪ The data center is not safe against natural and industrial accidents (for example, electrical failures, floods). ▪ A cloud service is used without having guarantees that the provider facilities are sufficiently protected.	☐ Yes ☐ No

Use of the processing system

Q6. Is there a lack of clarity in the roles and responsibilities of the employees? A lack of clarity in the definition of roles and responsibilities can lead to uncontrolled use of data (either accidental or intentional). Examples: ▪ A worker from a bank office should only consult the data of their clients. ▪ The personnel of the organization is responsible for destroying the information safely when no longer required. ▪ The personnel of the organization is responsible for maintaining the security of data when they communicate them to another person or organization.	☐ Yes ☐ No

Use of the processing system

Q7. Is there a lack of clarity in the definition of acceptable uses of the processing system? When acceptable uses of the processing system are not clearly defined, the risk of misuse is increased. Examples: ▪ The installation of file-sharing software can lead to involuntary file sharing. ▪ The installation of software by regular users (that is, users other than the system administrators) can lead to insecure configuration and poor maintenance. ▪ Visiting malicious webpages can be a source of malware and data theft.	☐ Yes ☐ No
Q8. Can the personnel connect external devices to the processing system? The connection of devices external to the treatment system is a gateway to the entry of malware, the introduction of vulnerabilities, etc. In addition, it also makes it easier for personnel to extract information. Examples: ▪ An employee connects a phone or a memory stick to the USB ports of the computer. ▪ An employee uses her device to perform processing tasks (BYOD).	☐ Yes ☐ No
Q9. Is there a lack of adequate procedures for registering and supervising the processing activities? The lack of a log of the activities (log file) can increase the bad practices of the personnel and, at the same time, hinders the investigation of the incidents once they have taken place. Examples: ▪ Patient records can be queried without access to the data being logged. ▪ Despite a log of the data processing activities carried out by each employee is generated, it is not monitored. ▪ Employees can access the data center without leaving a trail.	☐ Yes ☐ No

People

Q10. Do the personnel have permissions that are not necessary for the tasks assigned to them? The larger the number of people with access to some data, the greater the likelihood of abuse. To avoid this, it is essential to control the accesses of the personnel to the system and authorizes only those that are strictly necessary to perform their duties. Examples: ▪ Access to a patient's clinical history should be limited to the professionals who treat her.	☐ Yes ☐ No

People

Q11. Has some part of the processing been outsourced to a processor? Outsourcing the processing (or part of it) to a processor results in a loss of control over the data. It is the responsibility of the controller to choose a processor that offers the necessary level of security and defines the responsibilities of the processor clearly. Examples: ▪ A cloud is used to perform part of the processing. ▪ The controller lacks the knowledge to perform some data analysis and outsources it.	☐ Yes ☐ No
Q12. Does the personnel lack basic capabilities, attitude or knowledge regarding the proper use of the system and data security? The personnel of an organization is an essential part of any data processing performed by the organization. Personnel must have the necessary qualifications and attitude towards the job. A lack of knowledge by the personnel about the proper use of the system, about information security or about the obligations and limitations imposed by the RGPD can lead to bad practices that may put the security of the data at risk. Examples: ▪ A person that lacks basic knowledge about data security is more prone to act carelessly. For instance, by keeping sensitive data in a laptop device that is more prone to a thief and is unlikely to have a backup copy; or by following the instructions in a phishing email that seeks to gain access into the processing system.	☐ Yes ☐ No

Other characteristics

Q13. Has the organization or other organizations in the sector been attacked recently? The fact that an organization has suffered from previous attacks may indicate that attackers see the organization as an interesting target. Additionally, recent attacks suffered by other organizations in the same sector should also be a warning sign of potential attacks. Indeed, many attacks are conducted in campaigns. The reason is that when launching a new malware, attackers seek the greatest impact before people can react to it.	☐ Yes ☐ No
Q14. Have people complained about the stability or the security of the processing system? The presence of bugs in the processing system increases the likelihood of losing data, of altering data and, even, of suffering an attack. In the same way, notifications about potential security issues in the processing system should also be taken seriously.	☐ Yes ☐ No

Other characteristics

Q15. Are data of special interest or data of many users being processed? The presence of large amounts of data and the presence of especially sensitive data may be an extra motivation for attackers. Example: ▪ Ransomware encrypts the files in a system and then asks for a ransom to recover them. The greater the importance of the data, the more likely the attackers will get the ransom. ▪ An online store may keep the credit card information about their clients. Gaining access to such data may be an extra motivation for attackers.	☐ Yes ☐ No

Each affirmative answer to the previous questions indicates an increase in the probability of suffering data security incidents. To estimate the initial probability (without security controls), we count the number of affirmative answers and apply the following table:

Affirmative answers	**Initial Probability**
0 - 4	Low
5 – 9	Medium
10 - 15	High

Number of affirmative answers	
Initial probability	

4.3 Initial Risk

Once we have estimated the impact and the initial probability, we can compute the initial risk (that is, the risk without additional security controls). We use the same table that was used in section 2.6 Risks for the data subjects.

Impact over confidentiality Impact over integrity Impact over availability	
Maximum of the previous impacts Probability	
Initial risk	

4.4 Security controls

Once the initial risk has been calculated, it is necessary to determine which controls (measures to reduce risk) must be applied.

To plan the security controls, we need to use one of the standard lists of controls available. Otherwise, there is a high risk of missing important controls. There are many such lists. Although any (of the many standard lists available) should be fine, in this guide we use the ISO 27002.

A.5. Information security policies	
A.5.1 Management direction for information security	
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations	
A.5.1.1 Policies for information security	
The organization should define a set of policies for information security, which must be approved by management, published, and communicated to employees and external parties.	
A.5.1.2 Review for policies for information security	
The policies for information security must be reviewed periodically to make sure that they remain appropriate, especially in the case of significant changes in the system.	
A.6 Organization of information security	
A.6.1 Internal organization	
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.	
A.6.1.1 Information security roles and responsibilities	
Security responsibilities must be defined and assigned.	
A.6.1.2 Segregation of duties	
Duties must be segregated to limit the risk of misuse of the assets.	

A.6.1.3 Contact with authorities	
There should be a clear description of the authorities that need to be contacted in case of information security incidents.	
A.6.1.4 Contact with special interest groups	
Contact with information security professionals must be kept (e.g. to get security advice, to improve the security of the system, etc.)	
A.6.1.5 Information security	
In project management Information security must be present in all the phases of a project.	
A.6.2 Mobile devices and teleworking	
A.6.2.1 Mobile device policy	
The use of mobile devices introduces many risks (e.g. they may be lost or theft, users may install many applications, etc.). A policy regarding the use of mobile devices must be defined.	
A.6.2.2 Teleworking	
A policy must be defined to guarantee the security of the information processed when teleworking.	
A.7 Human resource security	
A.7.1 Prior to employment	
A.7.1.1 Screening	
Background verifications on candidates should be done in accordance with the business requirements and the perceived information security risks.	
A.7.1.2 Terms and conditions of employment	
The security responsibilities of employees should be stated in the contractual agreement.	

A.7.2 During employment	
A.7.2.1 Management responsibilities	
Management must require all employees to follow the security policies and procedures established by the organization.	
A.7.2.2 Information security awareness and training	
All personnel of the organization should receive periodic training on the policies and procedures relevant to their tasks.	
A.7.2.3 Disciplinary process	
A disciplinary process that targets employees that have committed information security breaches must be established and communicated.	
A.7.3 Termination and change of employment	
A.7.3.1 Termination or change of employment responsibilities	
The responsibilities with respect to information security that remain after change or termination of employment must be defined, communicated and enforced.	
A.8 Asset management	
A.8.1 Responsibility for assets	
A.8.1.1 Inventory of assets	
An inventory of the assets related to information or information processing must be maintained.	
A.8.1.2 Ownership of assets	
A person responsible for each of the previous assets must be appointed. This person must take care that the asset is properly managed throughout its entire lifecycle.	
A.8.1.3 Acceptable use of assets	
The use of information and information processing assets must be done according to a set of predefined rules.	

A.8.1.4 Return of assets	
Upon termination of employment, personnel must return all the assets of the organization in their possession.	
A.8.2 Information classification	
A.8.2.1 Classification of information	
Information assets should be classified in different categories according to their sensitivity (to unauthorized disclosure or modification), according to the criticality for the organization, and according to legal requirements.	
A.8.2.2 Labeling of information	
Information assets must be labeled according to the previous classification.	
A.8.2.3 Handling of assets	
The organization must develop procedures for handling the assets in the different categories of the adopted classification scheme.	
A.8.3 Media handling	
Objective: To prevent unauthorized modification, removal or destruction of information stored in media.	
A.8.3.1 Management of removable media	
The organization must establish procedures to manage removable media in accordance to the adopted classification scheme.	
A.8.3.2 Disposal of media	
Media must be securely disposed when no longer needed. When choosing the disposal procedure must take into account the classification of the information contained.	
A.8.3.3 Physical media transfer	
During transportation, media must be protected to preserve the confidentiality and the integrity of the information.	

A.9 Access control	
A.9.1 Business requirements of access control	
Objective: To limit access to information and information processing facilities	
A.9.1.1 Access control policy	
The organization must establish an access control policy to the information and the information processing facilities.	
A.9.1.2 Access to networks and network services	
Access to the network and the network services	
A.9.2 User access management	
A.9.2.1 User registration and de-registration	
A.9.2.2 User access provisioning	
A formal process for providing and revoking access rights to users must be implemented.	
A.9.2.3 Management of privileged access rights	
The assignment of privileged access rights must be limited and controlled.	
A.2.9.4 Management of secret authentication information of users.	
The allocation of credentials to users must follow a formal process that guarantees that the security of the secret authentication information is preserved.	
A.9.2.5 Review of user access rights	
The access rights of users to information and information processing assets must be periodically reviewed by asset owners.	

A.9.2.6 Removal or adjustment of access rights	
The access rights of users to information and information processing assets must be removed or suspended upon termination or change of employment.	
A.9.3 User responsibilities	
Objective: To make users accountable for safeguarding their authentication information.	
A.9.3.1 Use of secret authentication information	
Users must be required to follow the organization protocols for keeping the secrecy of authentication information.	
A.9.4 System and application access control	
Objective: To prevent unauthorized access to systems and applications.	
A.9.4.1 Information access restriction	
Access to information and information processing systems must be limited according to the access control policy	
A.9.4.2 Secure-log-on procedures	
Access to information and information processing systems must be protected by a secure log-on procedure.A.9.4.3 Password management system Quality passwords must be required.	
A.9.4.4 Use of privileged utility programs	
The use of software that can overcome the limitations set by security controls must be restricted and their use controlled.	
A.9.4.5 Access control to program source code	
Access to the source code of an application must be controlled to prevent unauthorized modifications and to keep the intellectual property safe.	

A.10. Cryptography	
A.10.1 Cryptographic protocols	
A.10.1.1 Policy on the use of cryptographic controls	
The organization must define a policy for the use of cryptography.	
A.10.1.2 Key management	
Cryptographic keys must be kept securely throughout their entire lifespan.	
A.11 Physical and environmental security	
A.11.1 Secure areas	
A.11.1.1 Physical security perimeter	
The required level of security of each area must be defined according to the sensitiveness of the information that contains.	
A.11.1.2 Physical entry controls	
Physical barriers must be implemented to prevent unauthorized access to secure areas.	
A.11.1.3 Securing offices, rooms and facilities	
The organization must design the facilities taking physical security into account (e.g. by preventing confidential information and activities from being visible from the outside).	
A.11.1.4 Protecting against external and environmental threats	
The organization must take into account physical disasters (such as fire, flood, etc.) when designing physical security.	
A.11.1.5 Working in secure areas	
Working in secure areas must be tightly controlled.	

A.11.1.6 Delivery and loading areas	
Areas where unauthorized persons can enter should be controlled and isolated from other areas where information is processed.	
A.11.2 Equipment	
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	
A.11.2.1 Equipment siting and protection	
Equipment must be protected to minimize the exposure to environmental threats and to unauthorized access.	
A.11.2.2 Supporting utilities	
Equipment should be protected from the failure of supporting utilities.	
A.11.2.3 Cabling security	
Cabling carrying power and telecommunications must be protected from any damage, interference, and interception.	
A.11.2.4 Equipment maintenance	
Equipment must be diligently maintained to prevent threats from happening.	
A.11.2.5 Removal of assets	
Information and equipment must not be taken outside the organization without a previous authorization.	
A.11.2.6 Security of equipment and assets off-premises	
The security of the assets that can be taken outside the premises of the organization must be designed taking into account the risks of working outside.	
A.11.2.7 Secure disposal or re-use of equipment	
Prior to disposal or re-use of an item of equipment, the organization must make sure that any confidential information present in the equipment and	

any software that gives access to confidential information have been securely removed.	
A.11.2.8 Unattended user equipment	
Users must be made aware of the risk of unattended equipment and make sure that they have the appropriate protection.	
A.11.2.9 Clear desk and clear screen policy	
The organization must establish a policy for clear desk and clear screen.	
A.12 Operations security	
A.12.1 Operational procedures and responsibilities	
Objective: To ensure the correct and secure operation of information processing facilities.	
A.12.1.1 Documented operating procedures	
Information processing activities should be documented, and those documents made available to users that need them.	
A.12.1.2 Change management	
Changes to the organization, processes, systems and facilities must be planned and the information security risks assessed.	
A.12.1.3 Capacity management	
The organization must make sure that it has enough resources (human, facilities, and equipment) to make sure that the system performs as expected.	
A.12.1.4 Separation of development, testing, and operational environments.	
The separation between environments limits the risks of security breaches in the operational environment. For instance, by excluding developers from accessing personal data in the operational environment, and by allowing the detection of security issues in the development or the testing environment.	

A.12.2 Protection from malware	
A.12.2.1 Controls against malware	
Effective protection against malware needs a combination of technical measures and personnel training.	
A.12.3 Backup	
A.12.3.1 Information backup	
Backup copies of the information, the software, and the systems must be done and tested regularly.	
A.12.4 Logging and monitoring	
A.12.4.1 Event logging	
User activities and system events must be logged, and the log reviewed to detect issues.	
A.12.4.2 Protection of log information	
Logs must be protected against unauthorized access and modification. In particular, against manipulation done by the system administrator.	
A.12.4.3 Administrator and operator logs	
The actions of the system administrator must be logged, and logs reviewed regularly.	
A.12.4.4 Clock synchronization	
To keep the consistency of logged events, the clocks of all systems must be synchronized.	
A.12.5 Control of operational software	
A.12.5.1 Installation of software on operational systems	
The installation of software on operational environments must follow previously defined procedures that take into account all security-related aspects.	

A.12.6 Technical vulnerability management	
A.12.6.1 Management of technical vulnerabilities	
Information about newly discovered vulnerabilities should be obtained regularly, the exposure evaluated and actions to protect against them taken.	
A.12.6.2 Restrictions on software installation	
Uncontrolled software installation introduces many risks: lack of updates, vulnerabilities not being monitored, etc. The organization must establish a software installation policy.	
A.12.7 Information systems audit considerations	
A.12.7.1 Information systems audit controls	
Audits of operational systems must be planned to minimize disruptions on the processes.	
A.13 Communications security	
A.13.1 Network security management	
Objective: To ensure the protection of information in networks and its supporting information processing facilities.	
A.13.1.1 Network controls	
Networks should be controlled to protect the connected systems and information.	
A.13.1.2 Security of network services	
The security requirements of network services and the mechanisms to meet them must be identified and included in network-service agreements.	
A.13.1.3 Segregation of networks	
The separation of a network into different domains improves security.	

A.13.2 Information transfer	
Objective: To maintain the security of information transferred within an organization and with any external entity.	
A.13.2.1 Information transfer policies and procedures	
Transfers of information should be done according to relevant policies and procedures. Controls must be put in place to guarantee that information transfers are appropriate.	
A.13.2.2 Agreements on information transfer	
The transfer of information between the organization and external parties must be done securely and following an agreement between the involved parties.	
A.13.2.3 Electronic messaging	
Electronic messaging systems must be secured (confidentiality, integrity, and availability).	
A.13.2.4 Confidentiality or non-disclosure agreements	
The organization identify the need for non-disclosure agreements and reviewed in a regular manner.	
A.14 System acquisition, development and maintenance	
A.14.1 Security requirements of information systems	
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems that provide services over public networks.	
A.14.1.1 Information security requirements analysis and specification	
Information security must be included in the requirements of new and in the enhancement of existing processing systems.	

A.14.1.2 Securing application services on public networks	
Information sent over public networks must be secured against fraudulent activity; such as inspection and tampering.	
A.14.1.3 Protecting application services transactions	
Services must guarantee that any transaction is complete, authentic and secured against unauthorized disclosure.	
A.14.2 Security in development and support processes	
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.	
A.14.2.1 Secure development policy	
The organization must establish a set of rules for the secure development of software within	
A.14.2.2 System change control procedures	
There must be a formal system for the control of changes; in particular, for major changes.	
A.14.2.3 Technical review of applications after operating platform changes	
A.14.2.4 Restrictions on changes to software packages	
Vendor supplied software must have as least modifications as possible.	
A.12.2.5 Secure systems engineering principles	
A set of security principles that must guide any development must be established.	
A.14.2.6 Secure development environment	
A secure development environment must be established. This should consider the people, the processes and the technology used.	

A.14.2.7 Outsourced development	
Outsourced development activities must be supervised.	
A.14.2.8 System security testing	
Security aspects should be present in testing.	
A.14.2.9 System acceptance testing	
System security should be one of the aspects to consider in system acceptance.	
A.14.3 Test data	
Objective: To ensure the protection of data used for testing.	
A.14.3.1 Protection of test data	
Test data should be carefully selected. In particular, the use of personal identifiable data must be avoided.	
A.15 Supplier relationships	
A.15.1 Information security in supplier relationships	
Objective: To ensure the protection of the organization's assets that are accessible by suppliers.	
A.15.1.1 Information security policy for supplier relationships	
A.15.1.2 addressing security within supplier agreements	
A.15.1.3 Information and communication technology supply chain	
Information security must be addressed in the agreements with suppliers.	
A.15.2 Supplier service delivery management	
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.	
A.15.2.1 Monitoring and review of supplier services	
The delivery of services by suppliers must be regularly monitored.	

A.15.2.2 Managing changes to supplier services	
Changes to supplier services must be managed according to their criticality and risks.	
A.16 Information security incident management	
A.16.1 Management of information security incidents and improvements	
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	
A.16.1.1 Responsibilities and procedures	
Responsibilities and procedures are essential to respond promptly and effectively to security incidents.	
A.16.1.2 Reporting information security incidents	
Personnel must be aware of the need and the appropriate channel to report information security incidents.	
A.16.1.3 Reporting information security weaknesses	
All personnel using the information processing systems of the organization must be required to notify observed or suspected weaknesses.	
A.16.1.4 Assessment of and decision on information security events	
Information security events must be assessed and escalated to security incidents when needed.	
A.16.1.5 Response to information security incidents	
The response to information security incidents must follow documented procedures.	
A.16.1.6 Learning from information security incidents	
The knowledge that results from the analysis of security incidents must be used to reduce the risk of new incidents.	

A.16.1.7 Collection of evidence	
Procedures to collect as much evidence as possible must be established.	
A.17 Information security aspects of business continuity management	
A.17.1 Information security continuity	
Objective: Information security continuity should be embedded in the organization's business continuity management systems.	
A.17.1.1 Planning information security continuity	
The organization must determine the information security requirements in case of a crisis or disaster. Unless otherwise specified, we must assume that information security requirements remain unaltered.	
A.17.1.2 Implementing information security continuity	
The processes, procedures, and controls to ensure that we keep the required level of information security during a crisis or disaster.	
A.17.1.3 Verify, review and evaluate information security continuity	
A.17.2 Redundancies	
Objective: To ensure the availability of information processing facilities.	
A.17.2.1 Availability of information processing facilities	
There must be enough redundancy in the information processing facilities and equipment to meet the availability requirements.	
A.18 Compliance	
A.18.1 Compliance with legal and contractual requirements	
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	

A.18.1.1 Identification of applicable legislation and contractual requirements	
All regulatory and contractual requirements must be identified. The approach of the organization to meet such requirements must be documented.	
A.18.1.2 Intellectual property rights	
Appropriate procedures must be put in place to ensure compliance with intellectual property rights.	
A.18.1.3 Protection of records	
Some records need to be maintained to meet legal or regulatory requirements. Such records must be appropriately protected against loss, unauthorized access, and unauthorized modification.	
A.18.1.4 Privacy and protection of personally identifiable information	
Personal data protection requirements in relevant legislation must be met.	
A.18.1.5 Regulation of cryptographic controls	
The use of cryptographic controls may be subject to external regulations. Relevant regulations must be met.	
A.18.2 Information security reviews	
Objective: To ensure that information security is implemented and operated in accordance with organizational policies and procedures.	
A.18.2.1 Independent review of information security	
Independent reviews of the approach to information security at regular intervals is necessary to ensure its effectivity.	
A.18.2.2 Compliance with security policies and standards	
The compliance of information processing systems with security policies and standards must be regularly reviewed.	

A.18.2.3 Technical compliance review	
Technical compliance with security policies and standards must be review regularly.	

4.5 Residual impact

Security controls can reduce the impact of a security incident. For example, encryption of certain information may limit the extent of a loss of confidentiality, backup may limit the impact of a loss of availability of information, and the use of electronic signature may allow for the detection of a loss of integrity (thus, reducing its impact).

Impact of a confidentiality breach (that is, of an unauthorized access to the data)

Impact

Low	Medium	High	Very high

Residual impact

Low	Medium	High	Very high

Justification

Impact of an integrity breach (that is, of an unauthorized modification of the data)

Impact

Low	Medium	High	Very high

Residual impact

Low	Medium	High	Very high

Justification

Impact of a loss of availability

Impact			
Low	Medium	High	Very high

Residual impact			
Low	Medium	High	Very high

Justification

The residual impact of the system is the maximum of the previous residual impacts.

Residual Impact of the system			
Low	Medium	High	Very high

4.6 Residual probability

To reduce the probability, we need to tackle the reasons why the questions in section 4.2 had an affirmative answer. For example, if allowing treatment over the internet is not essential, we can disable it to negate the answer to question P2.

Many times, it is not possible to completely eliminate all the reasons for having an affirmative answer. In this case, in order to change an affirmative answer to a negative one, we must justify that, in the context of the processing system, the implemented controls make the occurrence of security incidents a remote possibility.

Hardware and software

Q1	Is the processing system connected to external systems?	☐ Yes ☐ No
	Implanted controls and justification	
Q2	Is any part of the processing done through the internet?	☐ Yes ☐ No
	Implanted controls and justification	

Hardware and software

Q3	Is there a failure to follow a relevant good practices document in the design and the configuration of the processing system?	☐ Yes ☐ No
	Implanted controls and justification	
Q4	Is there a lack of following a relevant good practices document in the maintenance, monitorization and response to incidents?	☐ Yes ☐ No
	Implanted controls and justification	
Q5	Is there a lack of physical security in the processing facilities?	☐ Yes ☐ No
	Implanted controls and justification	

Use of the processing system

Q6	Is there a lack of clarity in the roles and responsibilities of the employees?	☐ Yes ☐ No
	Implanted controls and justification	
Q7	Is there a lack of clarity in the definition of acceptable uses of the processing system?	☐ Yes ☐ No
	Implanted controls and justification	
Q8	Can the personnel connect external devices to the processing system?	☐ Yes ☐ No

Use of the processing system

	Implanted controls and justification	
Q9	Is there a lack of adequate procedures for registering and supervising the processing activities?	☐ Yes ☐ No
	Implanted controls and justification	

People

Q10	Do the personnel have permissions that are not necessary for the tasks assigned to them?	☐ Yes ☐ No
	Implanted controls and justification	
Q11	Has some part of the processing been outsourced to a processor?	☐ Yes ☐ No
	Implanted controls and justification	
Q12	Does the personnel lack basic capabilities, attitude or knowledge regarding the proper use of the system and data security?	☐ Yes ☐ No
	Implanted controls and justification	

Other characteristics

Q13	Has the organization or other organizations in the sector been attacked recently?	☐ Yes ☐ No
Q14	Have people complained about the stability or the security of the processing system?	☐ Yes ☐ No
Q15	Are data of special interest or data of many users being processed?	☐ Yes ☐ No

We compute the residual probability according to the following table.

Affirmative answers	**Probability**
0 - 4	Low
5 – 9	Medium
10 - 15	High

Number of affirmative answers	
Initial probability	

4.7 Residual risk

Once we have estimated the residual impact and the residual probability, we can compute the residual risk (that is, the risk after the implementation of security controls). We use the same table that was used in section 2.6.

Residual impact over confidentiality Residual impact over integrity Residual impact over availability	
Residual maximum of the previous impacts Residual probability	
Residual risk	

If the residual risk is high, new controls need to be proposed to reduce it. If it is not possible to reduce it, we have to consult the competent data protection authority about the suitability of the processing before starting it.