ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

2022

SECURITY BREACHES OR LOSS OF INTEGRITY

ANNUAL REPORT

Index

List of Graphs

List of Tables

List of Figures

Executive Summary

ANACOM Security Regulation no. 303/2019 sets out the rules to be followed by companies providing publicly available electronic communications as regards the reporting of security incidents with significant impact: events that make access to the electronic communications service impossible for a large number of customers simultaneously and for a significant period of time.

In 2022, the downward trend in the total number of security incidents notified to ANACOM by electronic communications network and service companies continued: there were 37 security incidents, 1 fewer than in 2021 and the lowest figure recorded since 2015.

In contrast to the previous year, there was an almost uniform distribution in the number of incidents notified to ANACOM throughout 2022. The west coast region of mainland Portugal recorded the highest number of incidents in electronic communications networks and services.

In terms of root cause, "accident or natural phenomenon" was at the origin of most of the notifications received by the CRN in 2022. The root causes "maintenance or failure of hardware or software" and "failure to provide goods or services by a third party" in second and third place, respectively, represent over half the total number of reported security incidents (56%), especially resulting from situations associated with power failures, broken optical fibre cables, system/equipment malfunctions and scheduled outages for maintenance work.

Between 2015 and 2022, 74% of incidents were associated with factors external to the sector.

During the year, three types of incidents stood out: 23 incidents with a direct impact on networks and services and respective users, 5 incidents that affected the delivery of 112 emergency calls to public security service points (PASP) and 3 incidents with an impact on the operation of all networks and services offered by a company throughout the entire territory of an island in the Autonomous Region of the Azores.

Generally, most security incidents have a simultaneous impact on more than one publicly available electronic communications service. The fixed telephone service (FTS) was the most affected service, reported in 43% of all security incidents received, followed by the fixed Internet access service (IAS) with 38%, and the subscription television service (TVS) with 30%.

In 2022, these 23 security incidents had an impact on around 6.4 million subscribers, which is a very significant increase compared to 2021. This high number of affected subscribers is due to an incident occurring in February that had widespread impact on the networks and services of one of the main communications operators in Portugal, resulting from a cyberattack on its core network. This incident affected around 5.8 million subscribers/accesses.

The 23 security incidents reported in 2022 resulted in 360 hours of non-availability, which corresponds to an increase of 46% compared to 2021 (247 hours). The average duration per incident in 2022 increased by 33% compared to 2021, increasing from 12 to around 16 hours of impact.

Of the 37 security incidents recorded in 2022, eight incidents were identified as requiring provision of information to the public. This obligation applies when a security incident affects the operation of networks and services at one of the four most significant severity levels.

ANACOM reported five security incidents to the European Commission and to European Network and Information Security Agency (ENISA). European bodies are advised whenever an incident meets the more demanding reporting criteria at European Union level.

1 Introduction

This report compiles, presents and analyses information contained in notifications of security breach or loss of integrity with significant impact ("security incidents"). This includes data from “initial” notifications, "end-of-significant impact" and "final" notifications sent to Autoridade Nacional de Comunicações (ANACOM) in 2022 by companies offering public communications networks or publicly available electronic communications services in Portugal ("companies").

Under the terms of Article 60 of Law no. 16/2002 of 16 August ("Electronic Communications Law"), all companies are obliged to notify ANACOM of any security breach or loss of integrity whose occurrence has a significant impact on the operation of networks and services.

ANACOM approved the Regulation on the security and integrity of electronic communications networks and services ("Security Regulation No. 303/2019") by decision of 14 March 2019. However, ANACOM has had a CRN - Centro de Reporte de Notificações (Notification Reporting Centre) since 2014.

Companies are required to report security incidents to the CRN, providing information in real time on each occasion that a security breach or loss of integrity significantly affects the functioning of electronic communications networks and services. The CRN’s entry into operation has enhanced the systemisation and publication of security data in the sector.

As in previous years, in 2022, ANACOM submitted a report summarising notifications of security breaches or losses of integrity, as well as the measures taken[1].

Overall, in 2022, the trend in the total number of security incidents notified to ANACOM by companies continues to fall, with the number of notifications dropping to a new low. Although this continued downward trend is evidence of the sector's overall success in the adoption of appropriate measures to mitigate existing risks, the year being reported was marked by a single incident which had an enormous impact on the networks and services of one of the main communications operators in Portugal, resulting from a cyber-attack on the operator's core network.

In fact, this nationwide cyber-attack, which occurred in February, seriously affected fixed and mobile communications services. ANACOM kept in close contact with the company targeted

[1] In compliance with ENISA Technical Guideline on Incident Reporting Under The EECC, Version 2.*2,* March 2021, available at https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

by the attack from the outset, and liaised with other entities, including other National Regulatory Authorities, in order to assess possible impacts on other sectors (in cascade).

Given the increased likelihood of attempted attacks of this nature to communications networks and services, it is of the utmost importance that work on the adoption of preventive and mitigation measures is continued in a coordinated manner.

Section 2 presents an analysis of the incidents in terms of their distribution in time throughout the year, by root cause and according to their impact on the various services. Section 3 focuses on the circumstances giving rise to the obligation to notify, including impact levels and other rules, format and procedures, as well as the obligations to inform the public.

2 Security incidents in 2022

In accordance with paragraph 1 of article 21 of Security Regulation no. 303/2019 (“Circumstances”), a security incident must be notified when identified as a breach of security or loss of integrity that causes a serious disturbance to the operation of networks and services, with a significant impact on the continuity of such operation, according to the circumstances and rules provided for in paragraph 2 of this article. This means that not all episodes of degradation or breakdown of service are reported, but only those that reach certain thresholds or where other specified circumstances occur. Therefore, the information presented in this report, while giving an approximate and partial representation, is essential in order to ascertain and monitor trends in the robustness and resilience of electronic communications networks and services in Portugal.

The most relevant aspects and trends observed in the 2015-2022 period are reported below, and the volume and variety of occurring events is highlighted: trends in the number of incidents, intra-annual patterns, causality profile and impact on services.

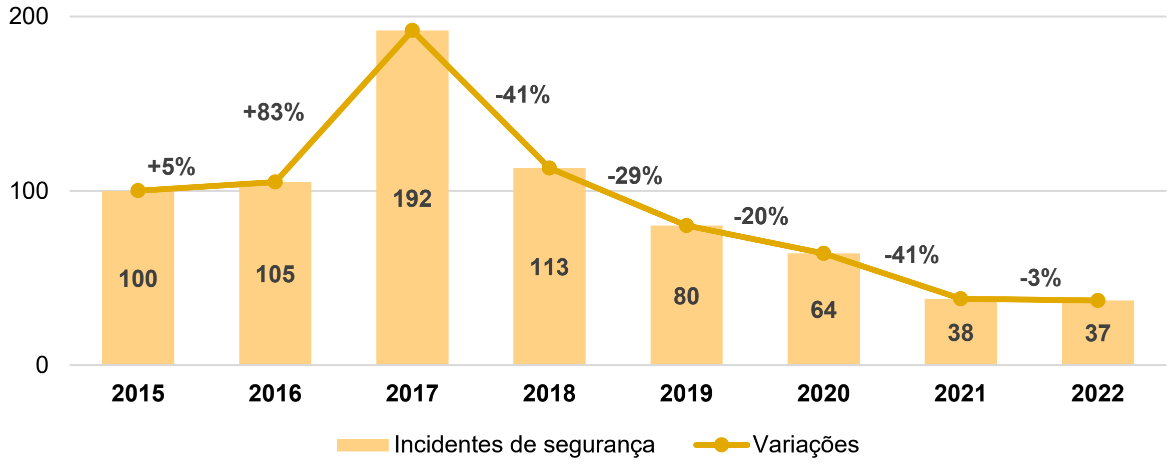
2.1 Number of reported security incidents

In 2022, companies communicated an absolute total of 37 security incidents to ANACOM.

This was the lowest number of occurrences since 2015. During the period 2015-2022, companies reported a total of 729 security incidents (annual average of 91 incidents).

Graph 1 shows a reversal of the initial upward trend in the number of security incidents notified each year, with a peak reported in 2017 (associated with that year's spate of serious forest fires) and then a progressive decline over the next five years.

Graph 1 – Volume and annual variation in notified security incidents, 2015-2022

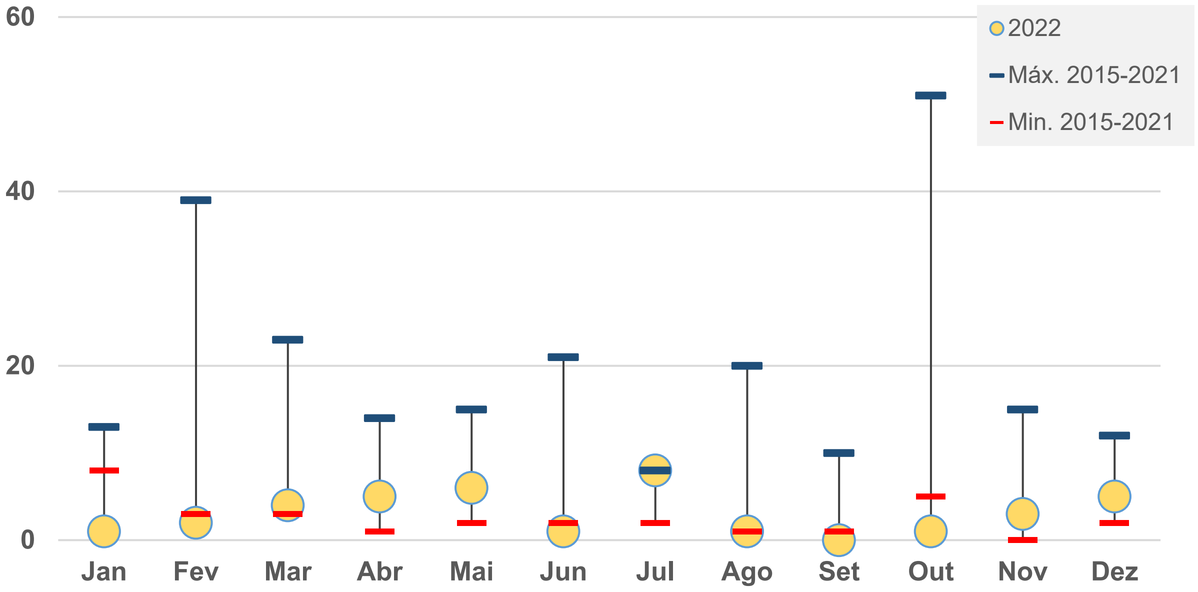


Unit: Number of security incidents

Source: ANACOM

Graph 2 shows the number of incidents received each month during 2022 compared to the maximums and minimums reported in the 2015-2021 period.

Graph 2 – Number of security incidents notified per month in 2022, compared to the period of 2015-2021



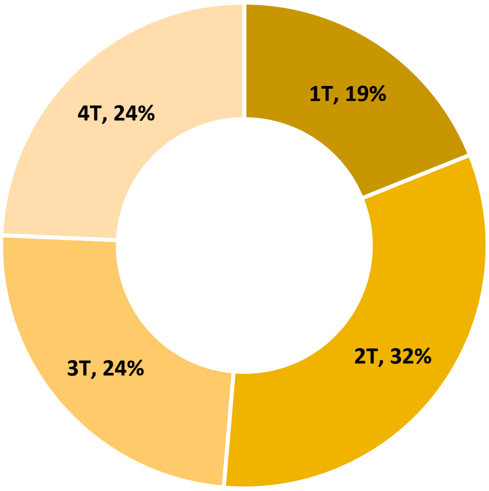
Unit: Number of security incidents

Source: ANACOM

As such, in 2022, the maximum value was recorded during the month of July (8 incidents) and a minimum value in September (zero incidents). In the last eight years, the maximum values for the number of reported security incidents were recorded in 2017 (39 security incidents in February and 51 incidents in October). In 2022, the months of June and September were among the months with the fewest incidents.

As seen in Graph 3, in contrast to the previous year, there was an almost uniform distribution of the number of incidents notified to ANACOM over the course of 2022, although the highest number of notifications was registered in the second quarter.

Graph 3 – Percentage of security incidents received in 2022, by quarter



Unit: % of security incidents
Source: ANACOM

2.2 Root cause

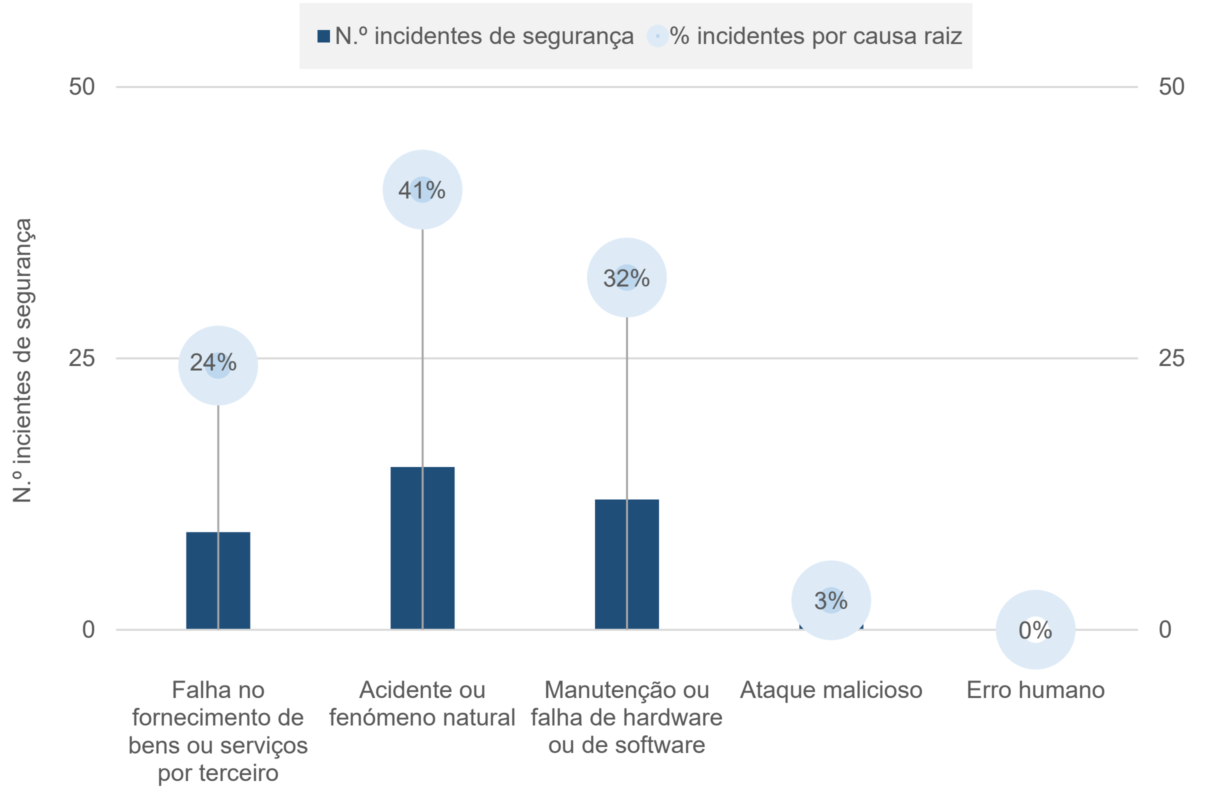
Under paragraph 11 of article 22 of Security Regulation no. 303/2019 (Formats and Procedures), security incidents are associated with the following categories of root causes:

- **accident or natural phenomenon** –severe weather conditions, earthquakes, floods, pandemics, forest fires, wildlife, etc.;
- **human error** – errors committed by employees of the company providing the service or its suppliers during the operation of equipment or installations, the use of tools, the execution of procedures, etc.;
- **malicious attack** – deliberate acts committed by a person or organisation;

- **maintenance or failure of hardware or software** – technical system failures in their physical (hardware) and/or logical (software) components;
- **failure to provide goods or services by a third party** –interruptions in the supply of goods or services, such as power or leased circuits, or any other good or service provided by third parties.

As shown in Graph 4, accidents or natural phenomena were the dominant root cause in 2022.

Graph 4 – Security incidents reported for different categories of root causes, 2022



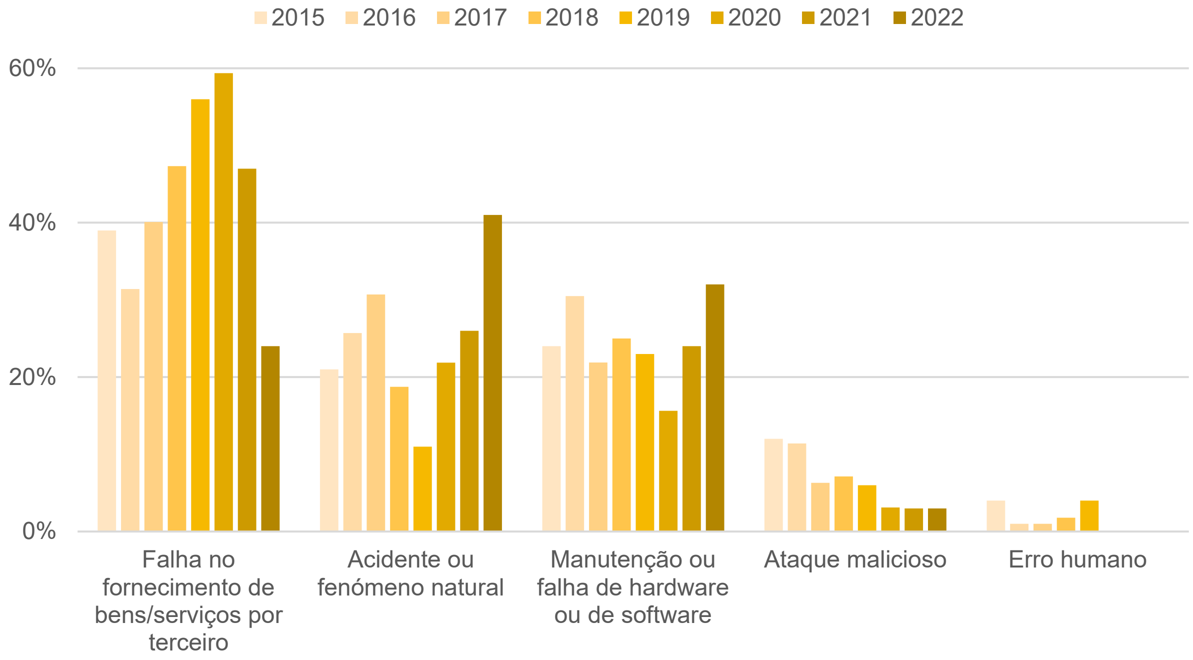
Unit: Number of security incidents and percentage of total incidents (%)
Source: ANACOM

In terms of root cause, "Accident or natural phenomenon" was at the origin of most of the notifications received by the CRN in 2022. The root causes “maintenance or failure of hardware or software” and “failure to provide goods or services by a third party” in second and third place, respectively, represent more than half of the total number of reported security incidents (56%), especially resulting from situations associated with power failures, broken optical fibre cables, system/equipment malfunctions and scheduled outages for maintenance work.

From Graph 5, it is possible to identify trends regarding the nature/root cause of the various security incidents. In 2022, the following trends were notable:

- reduction in the number of incidents associated with "Failure to provide goods or services by a third party";
- relative increase in the number of incidents caused by problems related to "maintenance or failure of hardware or software" and to "accident or natural phenomenon";
- the number of incidents resulting from "malicious attacks" (the only root cause of a deliberate or intentional nature) remained in line with the previous year;
- there were no incidents caused by "human error" (as in the previous two years).

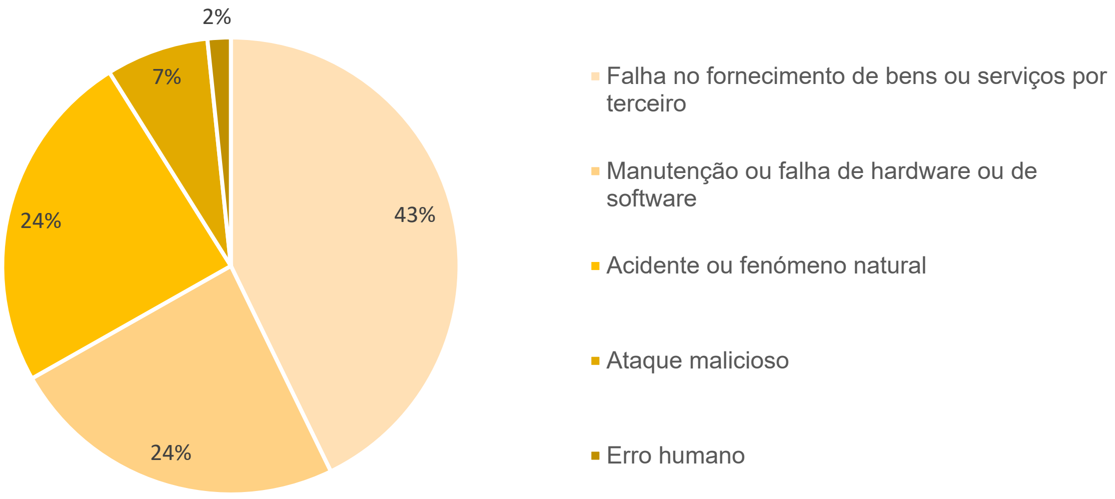
Graph 5 – Percentage of Security Incidents reported for each root cause, 2015-2022



Unit: % of security incidents
Source: ANACOM

Graph 6 clearly shows how the 729 incidents that occurred in the 2015 - 2022 period are distributed among the various root causes. "Failure in the supply of goods or services by a third party" continues to stand out in cumulative terms.

Graph 6 – Distribution of reported security incidents (729 in total) for each root cause, 2015-2022

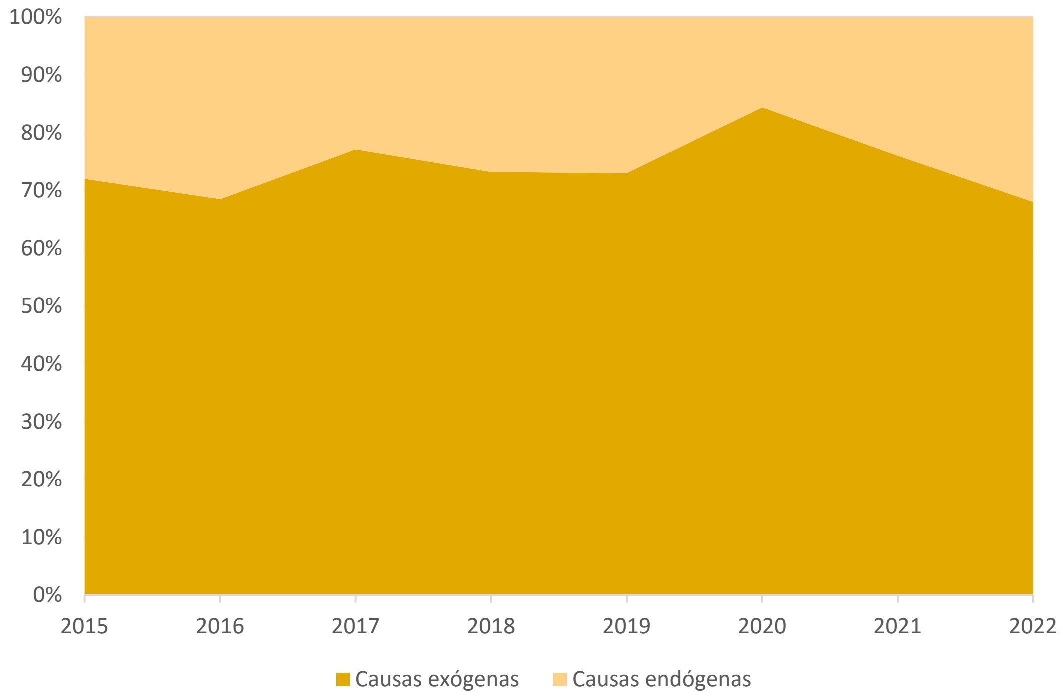


Unit: % of security incidents
Source: ANACOM

It is also possible to see the of division of incidents, for the 2015-2022 period, between exogenous causes (causes originating outside the communications sector - “Failure to provide goods or services by a third party”, “Accident or natural phenomenon” or “Malicious attack”) and endogenous causes (causes originating within the communications sector - “Maintenance or hardware or software failure” or “Human error”). For the entire period under analysis, 74% of incidents were due to exogenous causes and 26% due to endogenous causes.

Graph 7 shows the annual trend in this breakdown of causes, showing that exogenous causes tended to make up at least two thirds of incidents (ranging from a minimum of 68% in 2022 and a maximum of 84% in 2020).

Graph 7 – Distribution of root causes by exogenous and endogenous causes to the sector, 2015-2022



Unit: % of security incidents

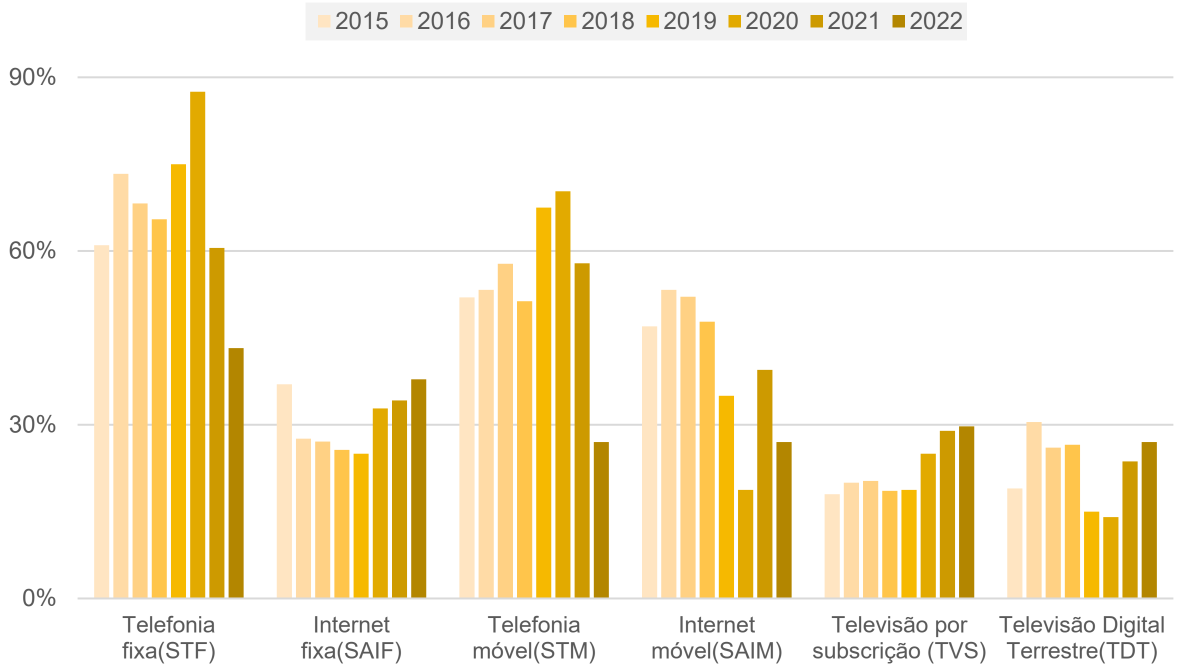
Source: ANACOM

2.3 Impact on services

Security incidents can affect one or more communications services electronic services, including, fixed telephone (FTS), mobile telephone (STM), fixed Internet access (FIAS), mobile Internet access (MIAS), subscription television (STV) and digital terrestrial television (DTT).

Graph 8 shows how the security incidents that occurred during the last eight years affected each individual service. The FTS and MTS were the most affected services throughout this period, in particular the FTS, which registered values above 60% every year except 2022. In 2022, there was a decrease in the number of security incidents notified with an impact on this service (43%); nonetheless the FTS remained the most affected service in that year.

Graph 8 – Percentage of security incidents reported for each type of service, 2015-2022



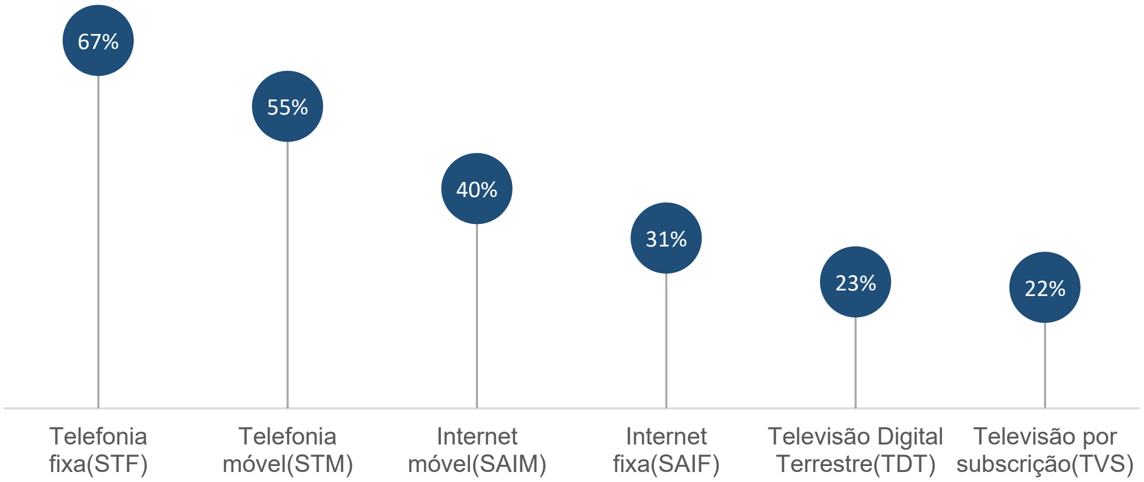
Unit: % of security incidents

Source: ANACOM

Note: The majority of security incidents impact more than one service (which is why the percentages in the graph add up to more than 100%).

During the last eight years it was found that the three most affected services were, in descending order (Graph 9): FTS (67%), MTS (55%) and MIAS (40%).

Graph 9 – Distribution of reported security incidents for each affected type of service, 2015-2022



Unit: % of security incidents

Source: ANACOM

3 Analysis of incidents in 2022

The circumstances that were at the origin of the notified security incidents causing a serious disturbance in the operation of networks and services, exceeding the significant impact thresholds established in article 21 of ANACOM's Security Regulation no. 303/2019, were as follows:

a) number of subscribers/accesses affected and respective duration of significant impact (a criterion that is divided into six levels depending on the number of subscribers/ affected accesses and duration of non-availability);

b) direct or indirect impact on the delivery of 112 calls to Public Safety Answering Points (112 Service Centres) for a period of 15 minutes or more;

c) impact on the operation of all networks and services offered by a company in the entire territory of an island of the Autonomous Region of the Azores or the Autonomous Region of Madeira, lasting 30 minutes or more (i.e. "isolated" islands[2]).

d) other circumstances set out in Article 21:

    i. impact occurring on a date when the normal and continuous operation of networks and services is particularly important (i.e., national election day - parliamentary, presidential, European or local elections);

    ii. cumulative impact of occurrences over a four-week period.

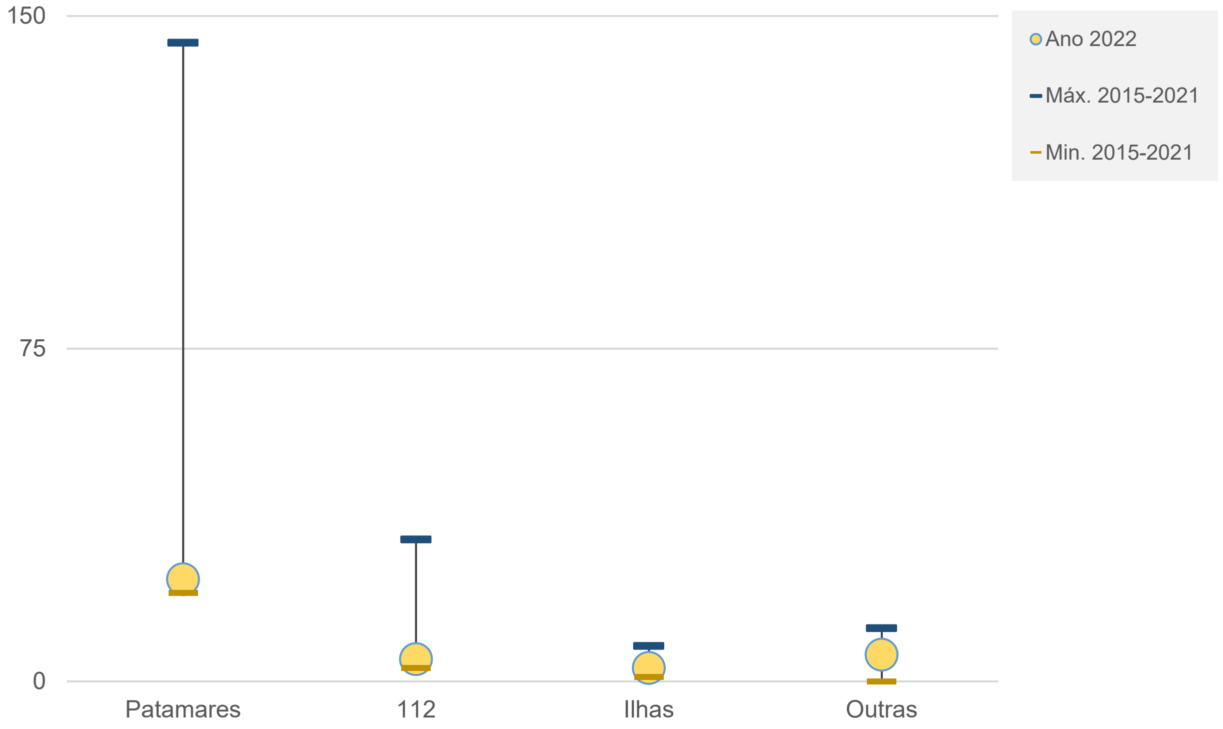
In 2022, there were security incidents with a direct impact on services provided to customers with an impact on the delivery of 112 calls to the PASP (point a)), impacting the entire territory of an island ("isolated" island) (point b)), and with accumulated impact over a four-week period - (point d) ii)).

3.1 Distribution of reported incidents

Graph 10 shows the number of incidents reported in 2022 and their distribution according to the circumstances established by Security Regulation no. 303/2019, and compares the maximum and minimum values in the 2015-2021 period.

[2] The circumstance of “isolated” Islands does not include incidents related to the 112 emergency service and corresponds to the classification of incidents that result in the failure of all networks and services offered by a company in part of the territory of an island.

Graph 10 – Security incidents reported in 2022 by circumstance, compared to the 2015-2021 period



Unit: Number of security incidents
Source: ANACOM

Of the 37 incidents occurring in 2022, there were 23 incidents from notifications that met the established impact levels (considering the number of subscribers/accesses affected and the duration of the impact), corresponding to 62% of the total number.

3.2 Affected Subscribers or Accesses (level)

Table 1 shows the six levels (from I to VI) corresponding to the levels of significant impact. These are defined by intervals of number of subscribers or affected accesses and duration of the incident. Level I is associated with the highest level of impact and level VI with the lowest.

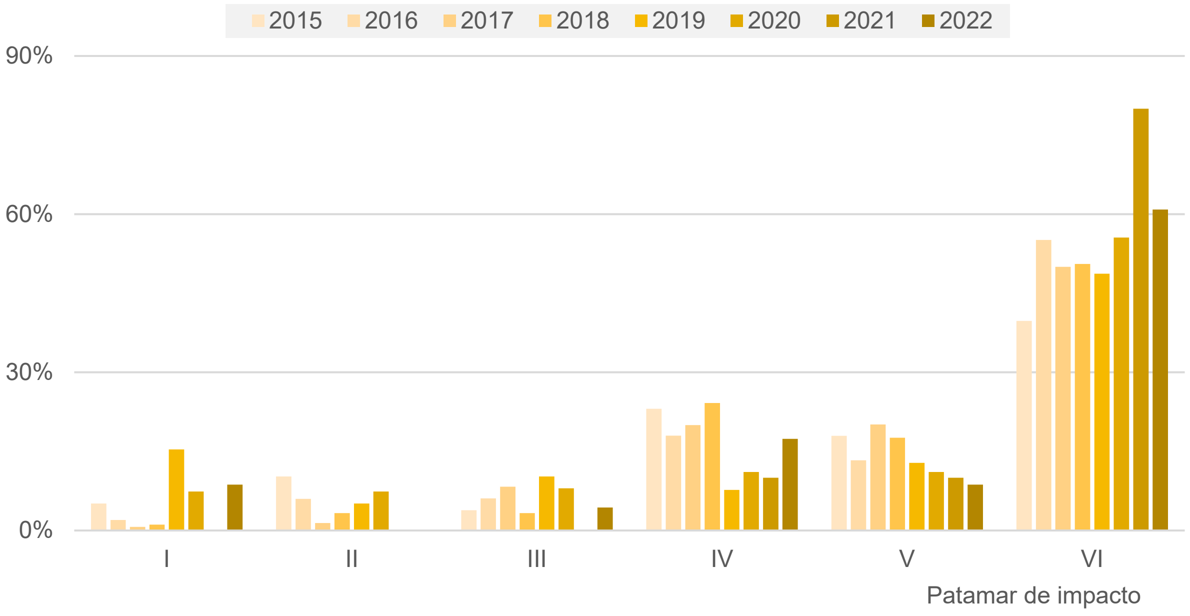
Table 1 – Levels of impact on subscribers/accesses

Duration, and	Number of subscribers or accesses affected [or, under the terms of point e) of paragraph 3 of this article, affected geographical area]	Level
≥ 30 minutes	number of affected subscribers or accesses ≥ 500 000 [or, under the terms of point e) of paragraph 4 of Section I, affected geographical area ≥ 3000 km$^{2]}$	I
≥ 1 hour	500 000 > number of affected subscribers or accesses ≥ 100 000 [or, under the terms of point e) of paragraph 4 of Section I, 3000 km^{2} > affected geographical area ≥ 2000 km^{2}]	II
≥ 2 hours	100 000 > number of affected subscribers or accesses ≥ 30 000 [or, under the terms of point e) of paragraph 4 of Section I, 2000 km^{2} > affected geographical area ≥ 1500 km^{2}]	III
≥ 4 hours	30 000 > number of affected subscribers or accesses ≥ 10 000 [or, under the terms of point e) of paragraph 4 of Section I, 1500 km^{2} > affected geographical area ≥ 1000 km^{2}]	IV
≥ 6 hours	10 000 > number of affected subscribers or accesses ≥ 5000 [or, under the terms of point e) of paragraph 4 of Section I, 1000 km^{2} > affected geographical area ≥ 500 km^{2}]	V
≥ 8 hours	5000 > number of affected subscribers or accesses ≥ 1000 [or, under the terms of point e) of paragraph 4 of Section I, 500 km^{2} > affected geographical area ≥ 100 km^{2}]	VI

Source: ANACOM, Security Regulation no. 303/2019

Graph 11 shows the number of notified security incidents for the 2015-2022 period, distributed by each of the levels mentioned above.

Graph 11 – Security incidents reported for each subscriber/access impact threshold (proportion), 2015-2022



Unit: % of security incidents

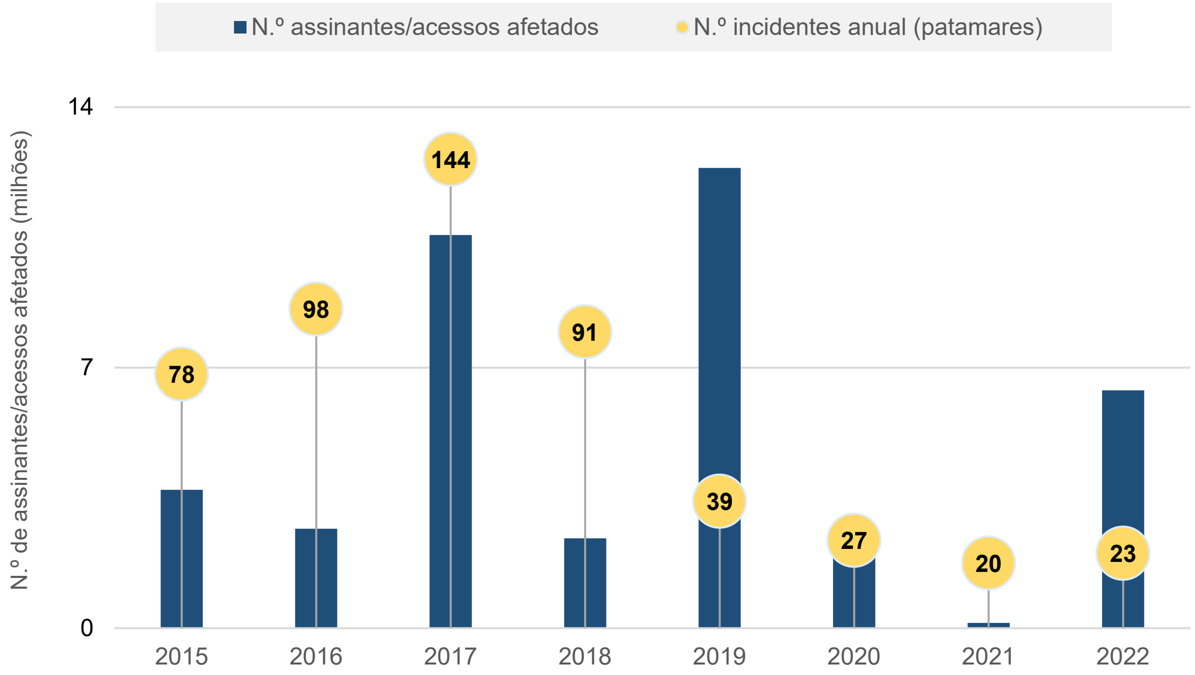
Source: ANACOM

In 2022, the lowest impact level (level VI) was the one with the highest number of associated security incidents (14 incidents in total).

Note is made of the relative weight of the number of incidents associated with the lower levels IV, V and VI, which, in the period 2015-2022, assumed an average weight of 87%.

Graph 12 shows the numbers of security incidents associated with each of the six levels of significant impact and the annual value of the total number of subscribers/accesses affected in the period 2015-2022.

Graph 12 – Security Incidents notified due to their impact on number of Subscriber/Accesses (levels), 2015-2022

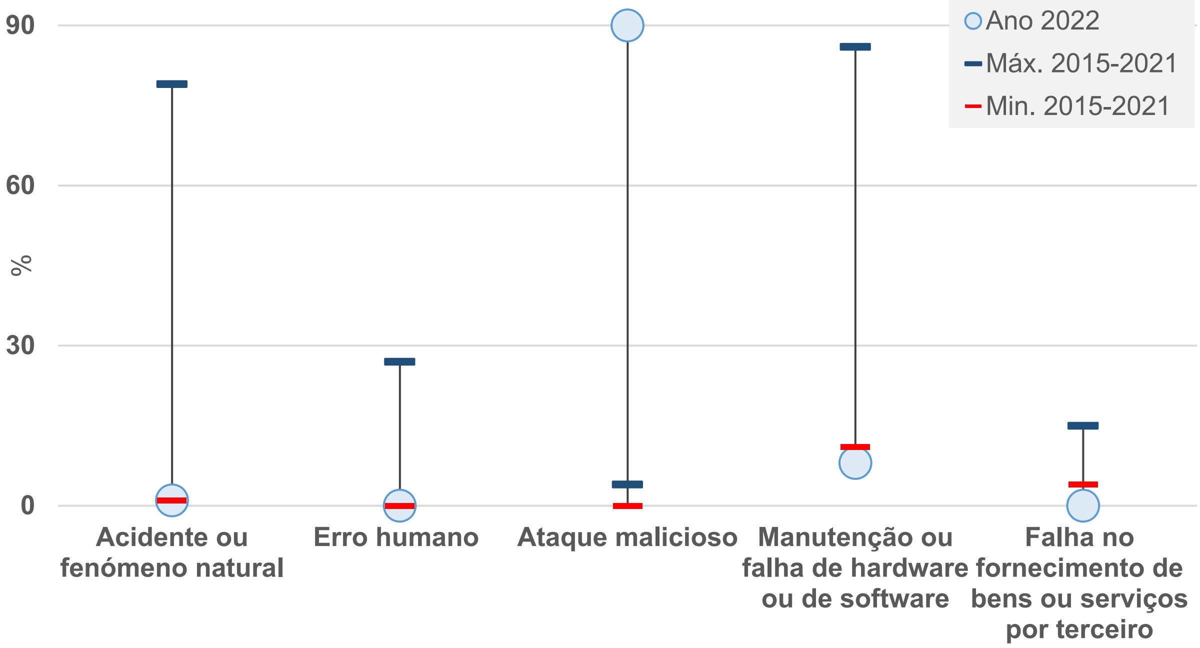


Unit: Number of affected subscribers/accesses (millions) and number of annual incidents (level)
Source: ANACOM

Comparing 2022 with the previous year, the total number of security incidents associated with the six levels of significant impact increased from 20 to 23 (an increase of about 15%). At the same time, there was an increase in the total number of affected subscribers/accesses from 144,467 to 6,391,934. This very significant increase is due to the cyber-attack (referenced above) on the core network of one of the main communications operators in Portugal.

Graph 13 shows the number of subscribers/accesses affected by root cause for 2022 and a comparison with the maximum and minimum values recorded in the 2015-2021 period. Note is made of the reduced percentage of incidents with “accident or natural phenomenon” and "maintenance or hardware or software failure" as root causes when compared to previous years. A large number of subscribers/accesses were affected by the root cause "malicious attack" (90%).

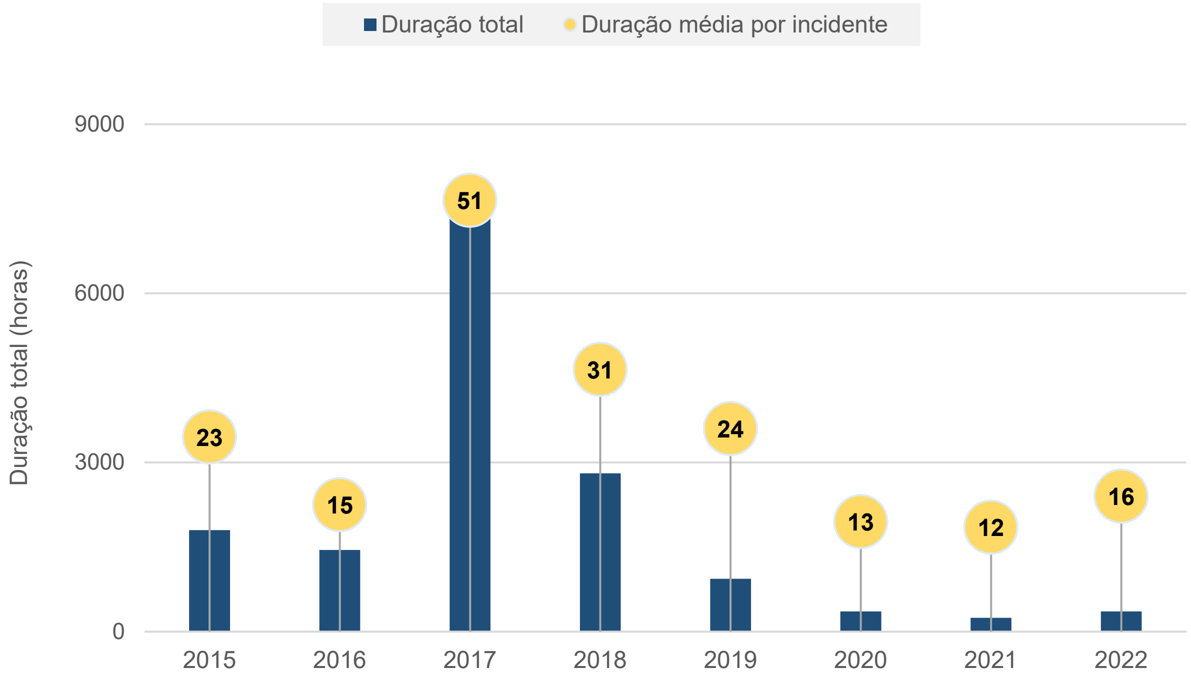
Graph 13 – Percentage of number of subscribers/accesses affected by root cause in 2022 compared to 2015-2021 period



Unit: Number of security incidents and number of subscribers/accesses
Source: ANACOM

In addition to the total number of subscribers/accesses affected each year, it is also important to analyse the accumulated annual duration of the impact caused by security incidents (annual duration of impact) and the average annual duration of impact of security incidents (average annual duration of impact). The latter set of data makes it possible to deduce an approximate value for the recovery time from security incidents. Graph 14 presents these values for the last eight years.

Graph 14 – Annual duration of impact and average annual duration of impact, 2015-2022



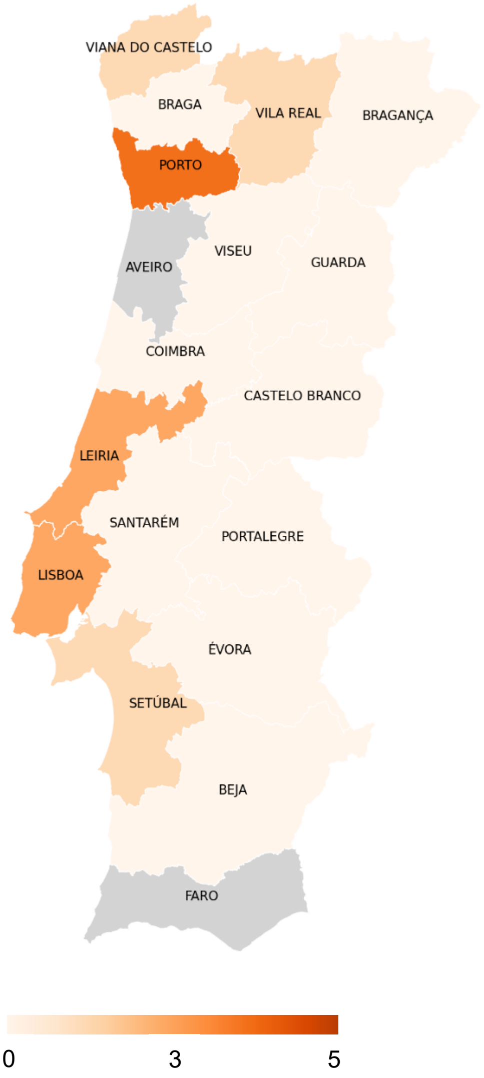
Unit: Hours
Source: ANACOM

In 2022, the total duration of impact was 360 hours, which corresponds to an increase of 46% compared to 2021 (247 hours). In both 2017 and 2018, there were long-lasting security incidents which resulted in a high value for the annual duration of the impact, a situation that has not been registered in the last four years.

The average duration per incident in 2022 increased by 33% compared to 2021, increasing from 12 to around 16 hours of impact.

Of the 23 security incidents, two were national in scope, while the rest had a significant impact on networks and services in the districts of mainland Portugal shown in Figure 1.

Figure 1 – Districts in Mainland Portugal affected by incidents with non-national scope notified in 2022



Unit: Number of incidents

Source: ANACOM

3.3 Calls to the 112 emergency number

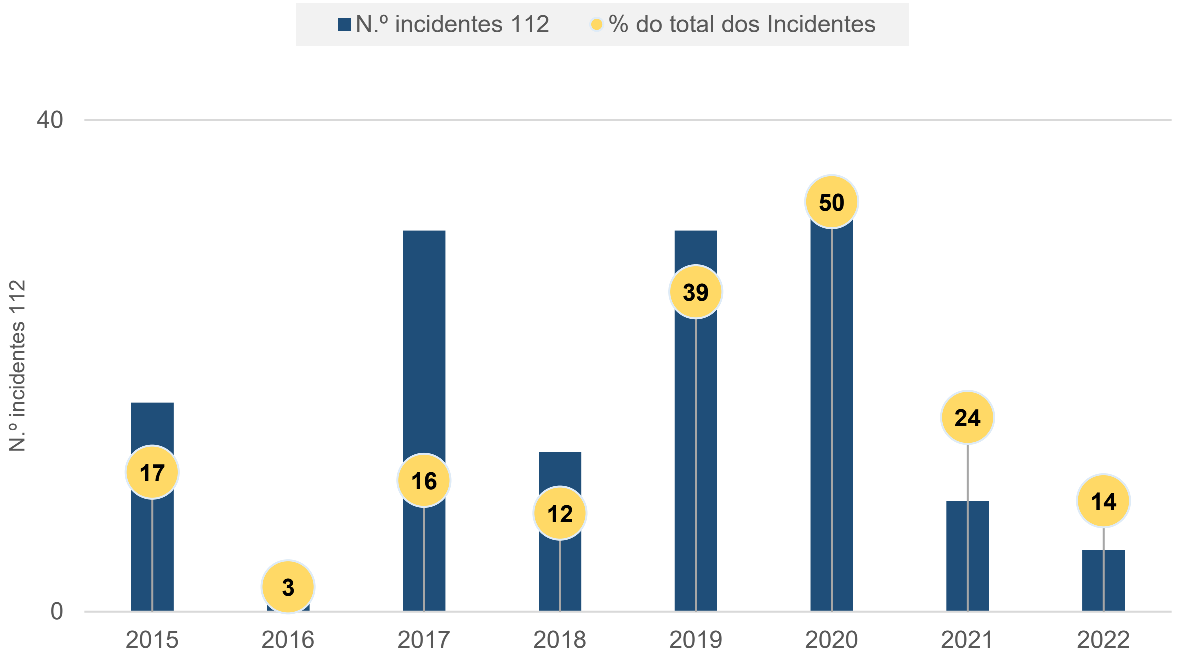
Companies are required to notify ANACOM of security incidents that directly or indirectly affect the delivery of calls made to the European 112 emergency number to PASP under point b) of paragraph 2 of article 21 of Security Regulation no. 303/2019, when incidents have an impact for a period equal to or greater than 15 minutes.

There are two separate situations: (i) situations of non-availability in accessing the 112 service, when the telephone service is available but it is not possible to connect the call to a PASP, (ii) situations where the telephone service itself is unavailable, making it impossible to make any call (to the 112 emergency number or to any other number).

It should be noted that in situations where a mobile operator's network is unavailable, it is possible to make an emergency call (112) using the available network of another mobile operator.

Graph 15 shows the trend, in recent years, in the number of incidents involving non-availability of access to the 112 service, as well as the percentage of this type of incident in relation to the total number.

Graph 15 – Notified security incidents associated with 112, 2015-2022



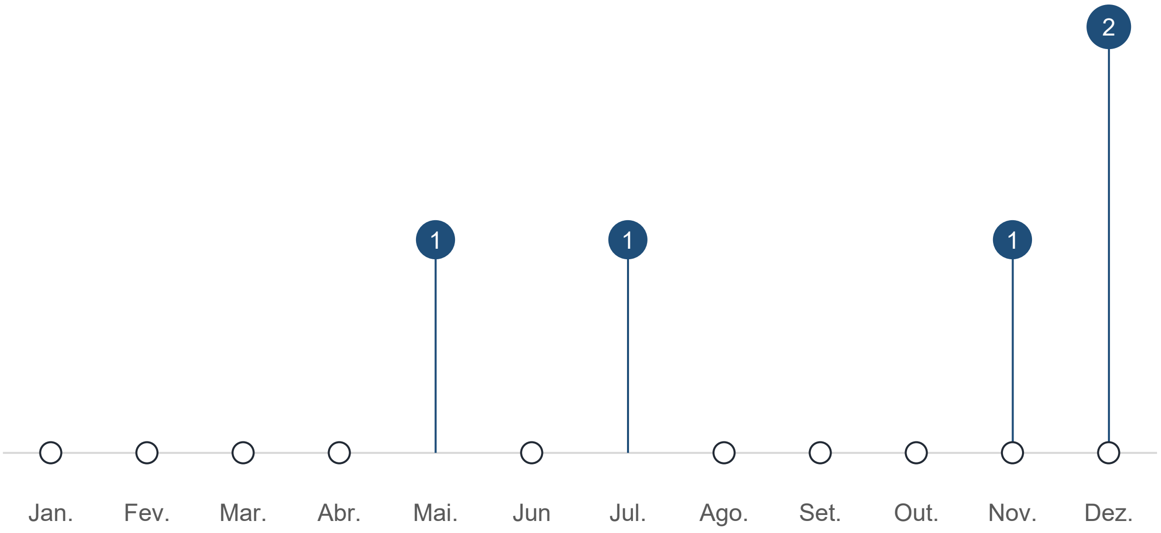
Unit: Number of security incidents and percentage of total incidents (%)
Source: ANACOM

In 2022, of the 37 security incidents that were notified, five of these had an impact on PASP access.

Occurrence of this type of security incident decreased in 2022 compared to 2021, in absolute numbers, from 9 incidents to 5 incidents, and, in percentage terms, from 24% to 14%.

Graph 16 shows the monthly distribution of the 5 security incidents related to 112 calls.

Graph 16 – Notified security incidents associated with 112 calls each month, in 2022



Unit: Number of security incidents
Source: ANACOM

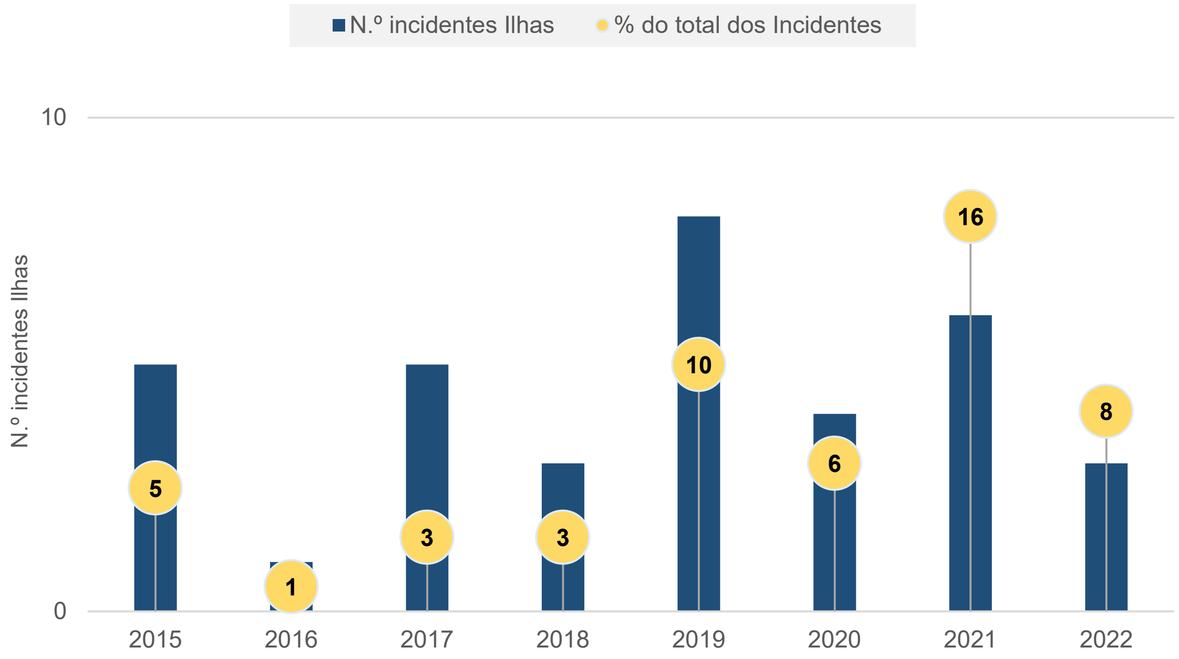
3.4 Islands ("isolated")

This section refers to security incidents in which all subscribers of a given operator are left without access to the electronic communications service within the entire territory of an island.

Under the terms of point e) of paragraph 2 of article 21 of Security Regulation no. 303/2019, companies are required to notify ANACOM of security incidents affecting the operation of all networks and services offered by a company throughout the territory of an island of the Autonomous Regions of the Azores or Madeira, provided that it lasts for a period of 30 minutes or more, regardless of the number of subscribers or accesses affected and the geographical area affected;

Graph 17 shows the 3 security incidents that occurred in the months of July, October and November 2022, which correspond to 8% of all incidents recorded in 2022.

Graph 17 – Notified Security incidents associated with the Islands criterion, 2015-2022

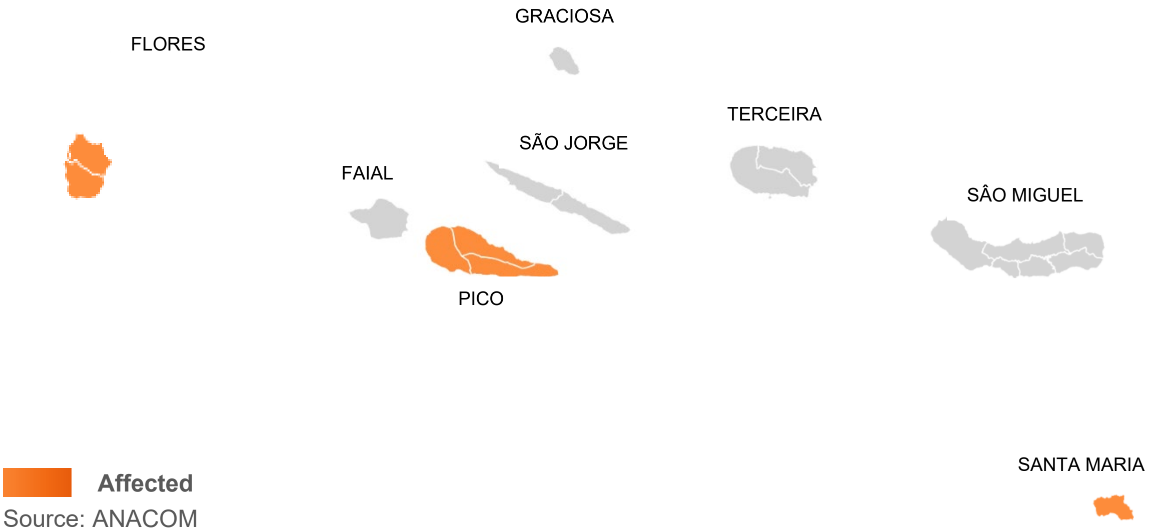


Unit: Number of security incidents and percentage of total incidents (%)

Source: ANACOM

Figure 2 identifies the islands where security incidents occurred with an impact on the operation of all networks and services (i.e., "isolated" island) offered by a company in the Autonomous Region of the Azores.

Figure 2 – "Isolated" islands of the Autonomous Region of the Azores due to security incidents, in 2022



Source: ANACOM

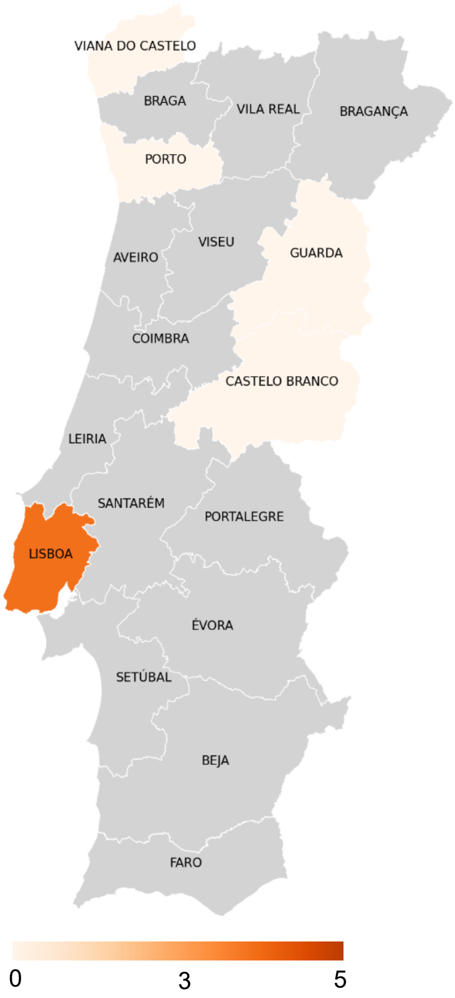
3.5 Other circumstances

In 2022, there were 6 recorded security incidents categorised under the other circumstances provided for in article 21 of Security Regulation no. 303/2019. These incidents were all due to cumulative impact of a breach of security or loss of integrity recurring over a period of four weeks.

Of all these security incidents, 5 had the root cause of “Maintenance or hardware or software failure” and 1 the root cause of “Accident or natural phenomenon”.

Figure 3 shows the affected districts where these 6 security incidents occurred.

Figure 3 – Districts in mainland Portugal impacted by incidents notified in 2023 in relation to other circumstances.



Unit: Number of incidents
Source: ANACOM

3.6 Information to the public

In accordance with the provisions of paragraph 1 of article 23 of Security Regulation 303/2019, companies are required to inform the public of any security incident whose impact on the operation of their networks and services is included in one of the following levels (Table 2):

Table 2 – Levels of obligation for companies to provide information to the public

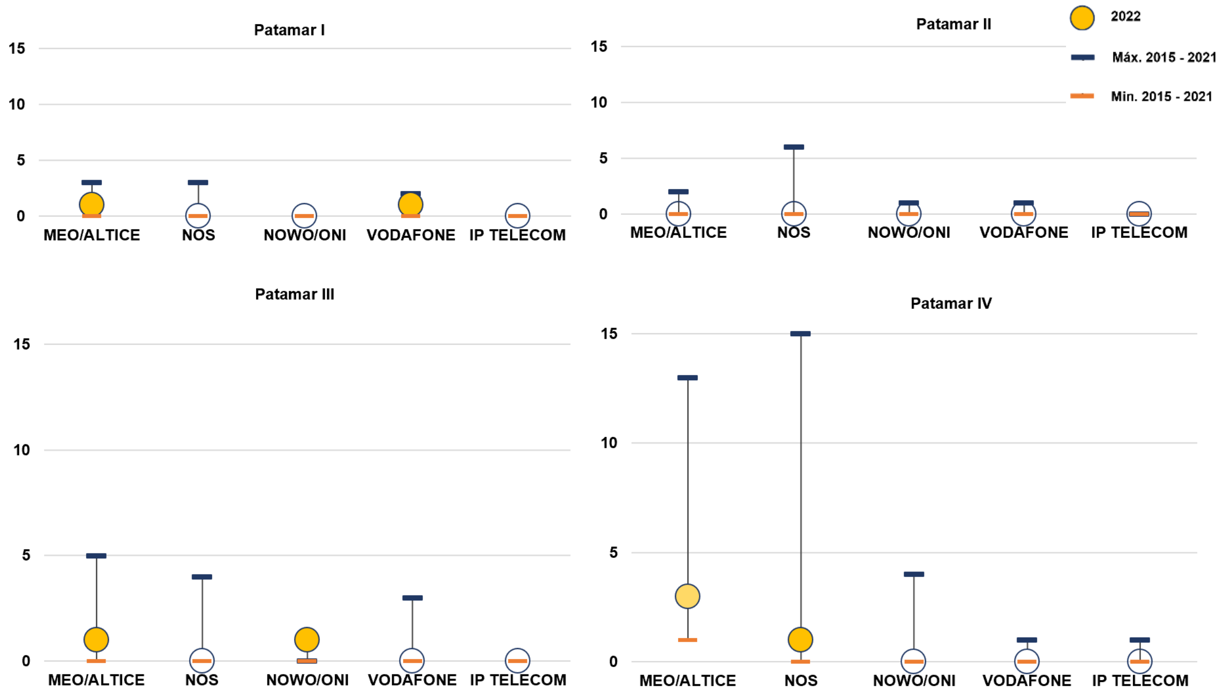
Duration, and	Number of subscribers or accesses affected or, under the terms of point e) of paragraph 2 of this article, affected geographical area	Level
≥ 30 minutes	number of affected subscribers or accesses ≥ 500 000 [or, under the terms of point e) of paragraph 4 of Section I, affected geographical area ≥ 3000 km^2]	I
≥ 1 hour	500 000 > number of affected subscribers or accesses ≥ 100 000 [or, under the terms of point e) of paragraph 4 of Section I, 3000 km^2 > affected geographical area ≥ 2000 km^2]	II
≥ 2 hours	100 000 > number of affected subscribers or accesses ≥ 30 000 [or, under the terms of point e) of paragraph 4 of Section I, 2000 km^2 > affected geographic area ≥ 1500 km^2]	III
≥ 4 hours	30 000 > number of affected subscribers or accesses ≥ 10 000 [or, under the terms of point e) of paragraph 4 of Section I, 1500 km^2 > affected geographical area ≥ 1000 km^2]	IV

Source: ANACOM, Security Regulation no. 303/2019

Information about a particular security incident is of interest, on most occasions, not only to subscribers directly affected, but also to all other users who have been prevented from communicating with them.

Of the 37 security incidents recorded in 2022, eight were identified for which information was provided to the public. Graph 18 shows the number of incidents of this type for each impact level and the respective comparison with the maximum and minimum values in the period 2015-2021.

Graph 18 – Security incidents where companies required to provide information to the public in 2022, compared to the period 2015-2021



Unit: Security incidents

Source: ANACOM

Under point c) of paragraph 1 of article 24 of Security Regulation no. 303/2019, the information must be made available as soon as possible and within a maximum period of four hours following initial notification to ANACOM.

Companies are required to make information available to the public, as a minimum on their websites with a hyperlink on the site's homepage, as provided for in point b) of the same paragraph 1. This link must immediately visible and identifiable without requiring use of the scroll bar, and the information must remain available to the public for 20 business days from the end date of the security breach or loss of integrity.

When it comes to the PASP, no information is made available to the public on the website, given that the 112 call centres are the responsibility of the Ministry of Internal Administration (MAI).

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

2022

Lisbon (Headquarters)
R. Ramalho Ortigão, 51
1099 - 099 Lisbon
Portugal
Tel: (+351) 217211000
Fax: (+351) 217211001

Porto
Rua Direita do Viso, 59
4250 - 198 Porto
Portugal
Tel: (+351) 226198000

Azores
Rua dos Valados, 18 - Relva
9500 - 652 Ponta Delgada
Portugal
Tel: (+351) 296302040

Madeira
Rua Vale das Neves, 19
9060 - 325 S. Gonçalo - Funchal
Portugal
Tel: (+351) 291790200

Public attendance
800206665
info@anacom.pt

www.anacom.pt