Summary
Olympic Games Rio 2016 .............................................................................................................. 1
1. Introduction ....................................................................................................................... 2
2. Brazil Geographic Location ............................................................................................ 2
3. Big Events in Brazil – Olympic Games Rio-2016 ............................................................... 3
4. Strategic Plan for Integrated Security .............................................................................. 6
5. SESGE .............................................................................................................................. 7
6. ABIN ................................................................................................................................. 8
7. Defense Ministry .............................................................................................................. 9
8. Overview on Cyber Threats in Brazil ............................................................................... 10
9. Issues During the Event ................................................................................................. 12
10. IT infrastructure of the Olympic and Paralympic Games Rio 2016 ................................. 12
11. Systems Integration Testing Laboratory .......................................................................... 14
12. Rio 2016 General Information ....................................................................................... 14
   Fans connected globally ....................................................................................................... 14
   Data Centers in the Rio de Janeiro ........................................................................................ 14
   Cisco UCS servers ................................................................................................................. 14
   Locations ................................................................................................................................ 15
   The Olympic Village ............................................................................................................ 15
   International Broadcast Center .......................................................................................... 15
   Main Media Centre ............................................................................................................. 15
   Network infrastructure and engineering services .............................................................. 15
   Planning, design and implementation support ................................................................... 15
Reference .................................................................................................................................... 16
1. Introduction

The Olympic and Paralympic Games Rio 2016 are the first held in South America and only the third below the equator after the 1956 Australian Olympics in Melbourne and in Sydney 2000.

The Rio-2016 event is considered the most connected event of all time and it is estimated that around 5 billion people around the world will attend the Olympic disputes. According to the data released by Canaltech\(^1\) Brazilian website, it is estimated that the official online media will account for 18 billion page views and nearly 3.5 billion videos are watched online, 1 billion visitors in the official pages of the event, 130 million hours videos watched on mobile devices and 170,000 hours of content produced and published almost in real time. All this information technology infrastructure began to be planned and designed almost 4 years ago, along with all aspects of cybersecurity.

Over the centuries XX and XXI, the Olympic Games were consolidated as a major cultural and sporting events on the planet and its organization demands direct involvement of the government and the private sector.

In one event of this magnitude, security, comprising public safety, national defence, intelligence, civil defence, urban planning and private security should be seen by a comprehensive perspective, which also covers actions to emergency services so that they are able to prevent and respond to threats which demand security and safety of the general population, the spectators, the delegations, delegations and guests for the event.

The main purposes of the present article are to show: What cybersecurity challenges did/does Brazil face in connection with these events? How do Brazilian authorities ensure cybersecurity for the events? Were lessons learned during past events fed into the preparation of the Olympics? Did Brazil cooperate with other countries to enhance cybersecurity for these events? What is the difference between past and future challenges in cybersecurity (more use of smartphones? New technologies? More users? Infrastructure increasingly digitalized.

2. Brazil Geographic Location

Brazil is the official name of the Federative Republic of Brazil. It is the largest country in South America and the Latin American region, and the fifth largest country in the world by land area (equivalent to 47% of South American territory) and population (over 200 million). It is the only country in America where Portuguese is the official language as well as being one of the most multicultural and ethnically diverse nations, due to the strong immigration from different locations around the world.

Bordered by the Atlantic Ocean to the east, Brazil has a coastline of 7491 km. It is bordered to the north by Venezuela, Guyana, Suriname and the French overseas department of French Guiana; northwest by Colombia; west by Bolivia and Peru; southwest by Argentina and Paraguay and on the south by Uruguay. Several archipelagos form part of Brazilian territory, such as Atol das Rocas, the Saint Peter and Saint Paul Archipelago Fernando de Noronha and Trinidad and Martim Vaz. The country shares land borders (a total of 15,719 km) with all other South American countries except Chile and Ecuador. Brazil is formed by the union of the Federal District, 26 states and 5570 municipalities.

3. Big Events in Brazil – Olympic Games Rio-2016

Since 2007, Brazil has been participating in Major Events that have occurred in various parts of the country, as Table 1. In Figure 1, you can have a preview of the Brazilian territory with the cities in which the Great Event occurred.

In October 2009, the International Olympic Committee announced the Rio de Janeiro as the host city of the 2016 Games.

The realization of the Military World Games Rio 2011, the Rio + 20 Conference, the FIFA Confederations Cup 2013 FIFA (FCC 2013), the World Youth Day (WYD) and FIFA World Cup 2014 (FWC 2014) allowed Brazil to accumulate expertise and to be ready to promote the 2016 Games safely.

The Brazilian Government had to sign the Candidature File to host the Olympics in 2016, the responsibility to coordinate the involvement of federal, state and municipal agencies in the Games security operation. It was created under the Ministry of Justice, the Special Secretariat Security for Major Events (SESGE), which established the Integrated Control and Public Safety Control for Major Events (SICC) and structured Integrated Centers of Command and Control (CICC) at national and regional level to support public safety initiatives in major events.

The Ministry of Defence created the Special Advisory Major Events, under the Joint Staff of the Armed Forces (AEGE / EMCFA), and used the Joint Operations Center (COC) as a framework for coordination and monitoring of the actions of the three armed forces. The Centers Area Defence Coordination (ADCC) worked at the regional level with the task of coordinating the constitutional authority of the activities of armed forces.

The Brazilian Intelligence Agency (ABIN), as the agency responsible for planning, implementation, coordination, supervision and control of intelligence activities in the country, centred participation component organs of the Brazilian Intelligence System (SISBIN) and coordinated the preparation of analyses of risk, the production of knowledge and the dissemination of information from the implementation of the National Intelligence Centre (CIN) and Regional Intelligence Centres (CIR) installed respectively in the ABIN headquarters in Brasilia and in the host cities.

The ABIN also mapped the hacker groups most likely to act in the event of the Olympics. Thus, members of this list groups work with a larger probability of attacks and they demonstrate a more advanced technical knowledge. The Agency worked closely with British authorities since the 2012 London Olympics.

The security operation for the World Cup 2014 FIFA demanded from the Brazilian Government, great efforts for its accomplishment. The flow of foreign tourists, for example, increased 196% in the period 09-21 of June 2014 compared to the same period last year. To meet these and other extraordinary demands, we employed approximately 177,000 professionals, 117,000 Public Security, 59,000 of the Armed Forces and 1,000 officers and intelligence agents.

The planning of public safety actions, defence and intelligence for the FIFA World Cup 2014 started from the premise that the ordinary demand security of the cities would be significantly impacted by the event, allowing the employed designed model to be left as a legacy to the cities.

Thus, one model will be largely replicated in the Rio 2016 Games, with the necessary adjustments to the characteristics of the Olympic event as the creation of sectoral centers in
each of the four Olympic areas (Barra, Copacabana, Deodoro and Maracanã) from the city of Rio de Janeiro.

The federal government and state and local governments involved are committed to ensure the safety of all guests of the Games, the local population and visitors before, during and after the Games Rio 2016. Governments will work in an integrated manner, with the objective to ensure safe and peaceful environment for the Games.

Given the complexity of the necessary actions to implement government strategies for the security of Rio 2016, Solid has established coordination between the Ministry of Justice (MJ), Ministry of Defence (MD) and the Institutional Security Cabinet (GSI-PR), to integrate security actions.

With the specific goal of holding the event in a peaceful and secure environment, the Strategic Plan for Integrated Security of Rio 2016 (SPIS) was published, which established the guiding principles, the concept of the Games security, the mission, situation, strategic goals to be pursued, the strategies to be used, the goals to be achieved, the actions to be implemented, the financial resources to be applied, the lines of action and governance to serve as guidance to the public security organs, defence national intelligence and develop their tactical and operational plans.

The SPIS (PESI is an acronym in Portuguese) (BRAZILIAN GOVERNMENT, 2015) is a dynamic character of the document and has been adapted to changes in the national and international scene.

The organization of Major Events, the Brazilian government used the structure of various ministries, with outstanding participation of the following: Office of Institutional Security, Ministry of Justice, Ministry of Defence, Ministry of Sports, Ministry of Culture, Ministry of Tourism, Ministry of Foreign exterior. However, for the various events were created institutions responsible for managing the planning and execution. In the aspect of security for Major Events Special Secretariat Security for Major Events (SESGE / MJ) was created, which will be more detail in SESGE item.

The Decree No. 7,682, of February 28, 2012 set the list of major events covered by the competence of the Security Special Secretariat for Major Events of the Ministry of Justice (SESGE) are: World Youth Day 2013; 2013 FIFA Confederations Cup; FIFA World Cup 2014; the Olympic and Paralympic Games of 2016; and other events designated by the President.

---

3 http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Decreto/D7682.htm#art1
Table 1 Big Events in Brazil - 2007 to 2016

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
<th>Host City</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>Pan-American Games</td>
<td>Rio de Janeiro</td>
</tr>
<tr>
<td>2011</td>
<td>the Military World Games&lt;sup&gt;4&lt;/sup&gt;</td>
<td>Rio de Janeiro</td>
</tr>
<tr>
<td>2013</td>
<td>FIFA Confederations Cup</td>
<td>Rio de Janeiro, Salvador, Fortaleza, Recife, Belo Horizonte and Brasilia</td>
</tr>
<tr>
<td>2013</td>
<td>World Youth Day&lt;sup&gt;5&lt;/sup&gt;</td>
<td>Rio de Janeiro and Aparecida do Norte</td>
</tr>
<tr>
<td>2014</td>
<td>FIFA World Cup</td>
<td>Rio de Janeiro, São Paulo, Fortaleza, Belo Horizonte, Brasilia, Porto Alegre, Salvador, Natal, Cuiabá, Curitiba, Manaus, Recife</td>
</tr>
<tr>
<td>2016</td>
<td>Rio 2016 Olympic Games&lt;sup&gt;6&lt;/sup&gt;</td>
<td>Rio de Janeiro, São Paulo, Belo Horizonte, Brasilia and Salvador</td>
</tr>
<tr>
<td>2016</td>
<td>Rio 2016 Paralympic Games</td>
<td>Rio de Janeiro</td>
</tr>
</tbody>
</table>

<sup>4</sup> http://www.milsport.one  
<sup>5</sup> http://www.vatican.va/gmg/documents/  
<sup>6</sup> https://www.rio2016.com/en
4. Strategic Plan for Integrated Security


The principles underlying the conduct of the institutions participating in the planning and implementation of safety actions of the Games are:

- Complementarity: the possibility of institutions with specific mandate to perform certain tasks to be supported by others, complementary and cooperative way, whenever circumstances require;
- Cooperation: joint efforts and interests to achieve goal, task, purpose or common mission. It is obtained through the harmony of distinct elements efforts aimed at achieving the same end, and avoiding duplication of efforts, resource dispersion and divergence solutions. To optimizes results, increases the effectiveness of actions and avoids mutual interference, which does not characterize subordination between the institutions;
- Discretion: to ensure low media coverage in the development of actions;
- Efficiency: ability of an operation to fulfill, properly and with economy of means, all planned assignments;
- Technical excellence: Training of the professionals involved to operate in a qualified way within international working standards and respect for human rights, taking advantage to do so, modern equipment and systems able to guarantee the provision of services at the highest level;
- Integration: joint action, articulated and coordinated between agencies, directly or indirectly, participate in safety actions, respecting the specific legal responsibilities of those involved;
- Interoperability: the ability of systems, units, forces and institutions to exchange information and services without compromising their functionality;
- Situational leadership: temporary situation that assigns a consensus basis, to an institution that has legal authority to fulfill certain task, coordination of integrated actions, respecting the powers of the other bodies involved; and
- Respect for diversity and human dignity: Constitutional foundation that ensures the exercise of social and individual rights and freedom of a fraternal, pluralist and unprejudiced society.

The SPIS considered the following items as major risk scenarios that could affect the safety operation of the Rio 2016 Games:

- acts of terrorism or sabotage of any kind;
- violent actions committed during social events;
- crime and urban violence;
- commitment of the urban mobility system;
- commitment of public health;
- Commitment of essential services;
- cyber-attacks;
- natural phenomena; and
IX. incidents and disasters.

To achieve the established objectives, the institutions shall use the following strategies:

a. To promote the integrated operation of the institutions from the planning stage to the final execution of the Games security actions, respecting the legal duties and promoting the rationalization of resources;

b. To develop and implement an integrated plan of public safety actions, national defense, intelligence and private security;

c. To establish integrated action protocols;

d. To strengthen the training structures of institutions;

e. To develop and use technological tools for integration of the agencies involved in the security actions;

f. To promote training activities and training necessary to achieve the security actions at the level of excellence and high degree of integration in planning and implementing actions;

g. To perform ongoing assessment of the planning, promoting any adjustments that may be required because of the lessons learned during testing events.

5. SESGE

To accomplish the task of coordinating the Public and Civil Defense Security actions during the course of the World Cup 2014 and the Olympic and Paralympic Games in 2016, the Ministry of Justice, with the support of the Ministry of Defense created the Safety of the Special Secretariat for Major Events (SESGE / MJ) in 2011.

The SESGE’s main scope of the agencies activity coordination involved in public safety and civil defense of the spheres of federal, state and local government, and the Brazilian State of the interface with the Organizing Committee of the FIFA World Cup Brazil 2014 and the Rio 2016 in private. The Special Security Secretariat for Major Events will be dissolved on July 31, 2017.

Security actions for Major Events include the coordination and planning of preventive operations and responses to risks, threats and incidents in the Operational Areas of Interest - AIO in the impacted areas or whose subject is of interest to Major Events and are the responsibility of the Ministry of Justice, through the SESGE / MJ.

In Great Events, security operations comprise all services that enable the smooth flow of the event schedule, emergencies and any serious incident or natural disaster that threatens the security of the population in general, game spectators, mega-event guests and delegations.

The Brazilian government, through the SESGE / MJ, promote public safety actions for Major Events, by strengthening Organs of Public Security, Defense, Intelligence, Civil Defense and Traffic Management at the three levels of government being based on criteria of promotion of human rights, integration of forces and the subsequent use of the developed infrastructure.

The team SESGE / MJ has heterogeneous profile. Its members come from various federal agencies of public safety, state and municipal. This feature provides the interaction of

---

7 http://www.justica.gov.br/sua-seguranca/grandes-eventos/grandes-eventos-1/sesge
professional knowledge with experience in security planning for major events, realizing, of course, the promotion of Integration and Cooperation.

6. ABIN

ABIN\(^9\) is the central organ of the Brazilian Intelligence System (SISBIN), whose strategic objective is to develop intelligence activities for the defence of the democratic rule of law, society, government effectiveness and national sovereignty. Among its duties, there is to evaluate the internal and external threats to the constitutional order, including cybernetics.

It has in its organizational structure, with the Center for Research and Communications Security Development (CEPESC), which seeks to promote scientific and technological research applied to communications security projects.

It is up to ABIN, as the body responsible for planning, implementation, coordination, supervision and control of intelligence activities in the country, centralizing the participation component organs of the Brazilian Intelligence System (SISBIN) and coordinate the development of risk analysis, production of knowledge and the dissemination of information from the deployment of intelligence centers.

The Brazilian Intelligence Agency (ABIN) mapped the hacker groups most likely to act on major events. The groups in this list work with larger scale attacks and demonstrate more expertise.

Also monitoring of several suspected work was carried out, which prevented more than 40,000 people interested in work, participate and even watch the Olympics. The work has intensified in recent weeks that preceded the start of the Olympics. The whole process had the support of various agencies of international intelligence as the CIA, the US Secret Service and the MOSSAD, the Israeli secret service, and the Russian intelligence, France, Germany and several Latin American countries.

The ABIN confirmed that at least 30 intelligence agencies maintained operations in Brazil and other 90 are part of a network of exchange of information of which Brazil is a member.

For the Olympic period, more than 110 intelligence agencies have been installed in Rio de Janeiro. This will be the largest security operation organized in Brazil and will have more than 80,000 agents only in Rio de Janeiro during the games. Of the total, about 10,000 will be granted by the National Force, which will act within the sports facilities.

Intelligence activities were coordinated by the Games Intelligence Center (CIJ) of the Olympic Games Rio 2016. The structure became operational on July 25 in oversight headquarters building of ABIN in Rio de Janeiro. The site housed professionals of 82 government agencies and utility companies (transport, water and energy, for example), attendance system and guard.

In CIJ, professionals of various public utilities and services agencies were meeting to exchange information on the security of the Olympics. The space also focused on monitoring of Intelligence actions performed in Rio de Janeiro. The main objective was to subsidize the axes defence and public security in the protection of the Olympic Games. From August 1 space operated full system, 24 hours a day. The ICJ was active until August 24. Between 5 and 20 of September, the centre will operate in support of the Paralympic Games.

\(^9\) http://www.abin.gov.br/
Brazil is not a country with a history of terrorist actions. However, the proximity of the Olympic Games Intelligence has detected Brazilian contacts with members of the Islamic State. Thus, Brazilian agencies focused efforts to identify terrorist cells in the country. Members of SISBIN received information that Brazilians living in the country were keeping contact with members of the Islamic State. The location, identification and monitoring of these people was the ABIN´s top priority. In the search for information on Brazilians who have come in contact with Muslim terrorist groups, SISBIN agents also keep in contact with the German federal police (BKA).

7. Defense Ministry

The major events in Brazil highlighted the importance of the Joint Armed Forces (EMCFA) in coordinating joint operations involving the Navy, Army and Air Force. The first integrated action of this magnitude happened in the Military World Games, held in 2011 in Rio de Janeiro. The event is organized every four years by the International Military Sports Council (CISM)\(^\text{10}\).

In 2012, the EMCFA led the security plan of the foreign delegations that came to the country to attend the UN Conference on Sustainable Development (Rio + 20).

In 2013, again the military jointly operated in the six host cities of the FIFA Confederations Cup, acting in the defence of strategic structures, air and sea space in cyber security, control of explosive and preventing terrorism.

Also in 2013, the Joint coordinated the participation of armed forces personnel in the security scheme of the World Youth Day (WYD), ensuring the integrity of the pilgrims and the Pope Francisco entourage, which, in addition to Rio de Janeiro, visited the city of Aparecida do Norte (SP).

According SPIS (BRAZILIAN GOVERNMENT, 2015), the use of armed forces in the Rio 2016 Games will take place within its constitutional mission and when to act on Law and Order guarantee this will happen by the disorderly presumption. They are exhausted instruments for preserving order public and the safety of persons and property related in art. 144 of the Constitution.

During the Olympics the structure of the Ministry of Defence will be organized from coordination composed by the three forces, which will be installed in Rio de Janeiro and in the five cities of football (Brasilia, Belo Horizonte, Salvador Manaus and São Paulo). In Rio, the Eastern Military Command took over the area of Defence General Command (CGDA), responsible for the actions in the Olympic areas Deodoro, Maracanã, Barra and Copacabana. The CGDA will be represented in all these regions by a Sector Defence Command (CDS).

Each of the cities football had an Area Defence Command (ADC). In addition, there was a command to each of the following: combating terrorism - which included DQBRN, security and cyber defence, aerospace and airport actions, supervision of explosives and military logistics.

Security actions and cyber defence activities, contributing to the protection of information assets, information and communications technology (ICT) systems of organized structures to coordinate security actions and cyber defence against threats arising from internal and external environments the country.

\(^{10}\) http://www.cism-milsport.org/eng/002_ABOUT_CISM/intro.asp
8. Overview on Cyber Threats in Brazil

With the proximity of Rio 2016, cybersecurity issues in Brazil attract worldwide attention for being considered one of the most connected events in history. The challenges in terms of cybersecurity in Brazil is unique compared to other countries. The cybersecurity issues are influenced primarily by technology, processes, people, environment.

Currently Brazil is one of the global players in cybercrime. The main threats are active bank fraud as in bank slips, remote access Trojans, and more recently, the ransomware has been gaining prominence on this list. The practices have been evolving and gaining sophistication as to be widespread, and the black market increasingly structured to sales tools to attack a service. The high financial returns due to the large volume of transactions and users connected, encourages new attacks against the banking sector.

According to the report, Fortinet, there was an increase of 200% in the number of intrusion attempts in Brazil, indicating that more cybercriminals are attacking, probably because of the Olympic Games in Rio de Janeiro. Looking at the graph, it is clear that the prevailing threats are very old and easy to perform. Most of them are related to scanning and brute force and DoS attacks.

![Figure 2 Q2 2016 IPS Events Brazil](source: Fortinet report)

This not to say that these are more dangerous attacks, but they are most commonly used by cybercriminals.

Some statistical indices of the Brazilian Cybercrime point to a difficult problem to solve. $ 8 billion in financial losses in 2015 and 6.6% of all financial cybercrimes in the world occurred in Brazil. Brazil occupies the 8th position among the countries with the highest malicious activity in the world and the 5th position among the countries with the highest traffic of malicious emails. Another thing that amazes experts is that Brazil has 33% of infected devices and it is responsible for 62.5% of e-mails identified as spam volume in 2015.

In Brazil, CERT.br is Responsible for handling computer security incident reports and activity related to networks connected to the Brazilian Internet. The CERT.br is the Brazilian National

---

12 [http://goo.gl/OQNQnV](http://goo.gl/OQNQnV)
Computer Emergency Response Team, maintained by NIC.br - the executive branch of the Brazilian Internet Steering Committee. The CERT.br keeps statistics on notifications of incidents reported to it. Thus, based on data CERT.br major incidents reported from January to December 2015 are: Scan (54.17%), worm (6.61%), Web (9.09%), invasion (0.34%), DoS (3.51%), Other (2.91%) and fraud (23.37%). A more detailed analysis can be obtained at (CERT.BR, 2015)

According to the report of the company Trend\textsuperscript{14}, Latin America is a place that facilitates rapid rise for cybercriminals, mainly in Brazil. A recent finding is the approach of Brazilian cybercriminals with criminal groups in Eastern Europe. This approach encourages new attacks because of the use of infrastructure in other countries and a high return caused by the volume of transactions.

In Brazil, the online banking transactions are their biggest target, becoming prevalent banking malware. Attacks aimed at bank slip and on-line payments are a feature of the country, and organized crime has been structured to cover especially these types of transactions. This peculiarity is characterized by actuation so that after infecting the machine, billet handles data before reaching the bank, without relying on human performance and acting in different web browsers.

According to the electronic magazine Computer World\textsuperscript{15}, in Brazil, there are 42 million Internet users and Banking, according to FEBRABAN\textsuperscript{16}, the market has accumulated losses of R $ 1.4 billion in the year 2012. Each R $ 100 stolen or stolen from Brazilian banks at least R $ 95 were via electronic fraud made by Internet banking or cards. Because of the continuing popularity of online bank in the country, there is a proliferation of banking malware.

Brazilian cybercriminals are less dependent on the Deep Web and have little regard for police. The audacity of the criminals will let you take their operations to the "Surface Web". For $ 3,000 dollars or 9 bitcoins, cybercriminals can use an unlimited number of ransomware platform within a week. This facility has initiated a new type of cybercrime, "ransomware as a Service".

In Brazil there are 255.2 million of mobile devices and the Brazilian preference for devices with Android system. Much of the mobiles present in Brazil are prepaid, which you need to purchase phone credits before use. Prepaid credit for mobile greed are targeted by criminals. In addition, Brazilians are in large numbers on social networks like Facebook and Twitter and others. As a result of this phenomenon, many Apps for Android also recently appeared in the Brazilian underworld. They were set up to pay for prepaid credits with credentials of stolen credit cards. This appearance of offerings in the underworld can be attributed to the high penetration rate of mobile devices in Brazil (142% up to April 2015).

Teleco\textsuperscript{17} site provides the data communications media in Brazil and worldwide. By comparison, Brazil has more mobiles than the UK, Germany and France together, according to data from 2015. Table 2 are available telecom data in Brazil.

\textsuperscript{15} http://computerworld.uol.com.br/
\textsuperscript{16} febraban.org.br
\textsuperscript{17} http://www.teleco.com.br/
Brazilian cybercriminals have also begun to offer services involving the theft of personally identifiable information from victims that they can then sell to others by 0.015 BTC (US $ 6.81 *). Personally identifiable information stolen can be hacked or come databases compromised as CadSUS\(^{18}\) (Join the Unified Brazilian Health).

### 9. Issues During the Event

The Olympic Games attract the attention of many people - including cybercriminals. According to information disclosed by CIO magazine\(^{19}\), the environment faced a massive amount of hacker activity, with over 40 million security alerts, which generated approximately 25 million attacks, triggering 223 mitigated actions. However, despite the amount of attacks, none of these incidents detracted from performance technology.

As stated by the subject of the magazine, the Olympic Games amount to an operation of an IT company with 200,000 employees and serves 4.8 billion customers 24 hours a day seven days a week. This operation can be said for a short time and with different peak times the volume of access systems.

This was the first time the Olympics will run cloud IT management systems\(^{20}\). Among the tools moved to the cloud were the volunteer portal - which was carried out the recruitment of 70,000 people - and the accreditation system that focused management 300,000 credentials. In London, the company Atos worked with 700 physical servers in Brazil are 250.

The use of cloud computing resources was considered one of the highlights of 2016, as the first Olympics to use this technology. Perhaps the biggest challenge was the operation for a few days, but of great intensity. The model brought scalability and agility to provision according to demand technology environment. As an example, the portal of 2016 was provided by 300 virtual servers on Microsoft Azure platform distributed in four data centers on three continents. The system recorded 636 pages displaying peaks per second, with over 4.7 million concurrent users. In all, 47 million visitors, which generated more than 91 million consultation sessions with over 470 million page views.

### 10. IT infrastructure of the Olympic and Paralympic Games Rio 2016

The 2016 was the most connected event in history\(^{21}\). This finding brought many challenges for the organization of the event. Four years ago in London, Snapchat did not exist and the streams

---

\(^{18}\) datasus.saude.gov.br

\(^{19}\) http://cio.com.br/noticias/2016/08/25/exclusivo-sistema-da-rio-2016-enfrentou-25-milhoes-de-ataques-de-seguranca/

\(^{20}\) http://computerworld.com.br/node/53871

were limited to little-known platforms. We currently have smartwatches, smartphones connected to the 4G network, dozens of social applications. The media outlets transmit photos in Full HD images in 4K or 8K and even in virtual reality. All these were taking into account to provide content to 5 billion people around the world. According to ratings, 5 out of 7 people in the world will be affected by 2016.

The Olympic and Paralympic Games Rio 2016 counted 1,000 cameras to generate the transmission of images during the days of the Games. Olympic Broadcasting Services (OBS) an agency of the IOC will feature 7,000 professionals who work in broadcasts that reached about 5 billion 200 countries viewers. The OBS was responsible for generating more than 7000 hours of transmission, who attended the broadcasters holding the rights in countries around the world. The sporting event was covered about 25 000 journalists and support of 10,000 volunteers.

América Móvil\textsuperscript{22} Group invested R$30 billion in Brazil in the past three years, with targeted investments in the communications infrastructure of the Games. America Movil, which controls the companies Claro, Embratel and NET.

According to the group, it will use the entire infrastructure of their installed companies in the country, including more than 181,000 kilometers of optical cables, 17,000 km of submarine cables, 17,000 base stations (Radio Base Stations for Mobile), 8 satellites in orbit and 5 data centers. The basic telecommunications in 2016 was the Backbone Olympic Embratel - network of over 370 km of optical fibers which ensured high availability in game data transmission. The Olympic network has speed of 40 Gbps, connecting more than 60,000 access points spread across more than one hundred sites related to the event. Embratel provided the fiber optic network that was used to capture video signals of the competitions of the Olympic Games, delivering them to the IBC broadcasting center (International Broadcast Centre), location where they will be distributed images to approximately 5 billion viewers in at least 200 countries.

Under the responsibility of Technology Operational Center (TOC) was the management of the network and the services offered. The TOC is designed to work continuously during the event, and about 3000 professionals Claro, Embratel and NET worked in the Games.

They were installed 97 3G broadcast stations and 4G mobile network company Claro, which gave stand the increased use of mobile phones at the time. The company also offered another 20 thousand lines of mobile phone to meet the participants of the sporting event organization in Brazil. The company NET released 12,000 pay TV spots, 10 000 fixed telephone lines and 8000 points of Wi-Fi properly throughout the city of Rio de Janeiro.

Cisco company is supportive and official supplier of the Olympic and Paralympic Games Rio 2016, responsible for the Network and Enterprise Servers equipment. The company provided Cisco UCS servers of blade and rack families. Cisco also provided the network infrastructure for the event, including all the wired and wireless LAN networks, IP routers, network security solutions, data center networks and network management systems.

The company started producing in Brazil rack servers and blade UCS family system that unifies computing, networking, management, virtualization and storage access into a single integrated

\textsuperscript{22} http://canaltech.com.br/noticia/olimpiadas/rio-2016-contara-com-1000-cameras-para-gerar-imagens-de-transmissao-69145/
architecture. Announced in 2012\textsuperscript{23}, Cisco’s investment plan in Brazil included the expansion of local manufacturing production UCS.

11. **Systems Integration Testing Laboratory**

From April 8, 2014\textsuperscript{24}, the International Olympic Committee (IOC) began delivering the first concrete initiatives in terms of information technology for Rio 2016. On a global partner with Atos, the agency opened the Integration Test Lab (ITL or Integration Testing Laboratory) of the Olympic and Paralympic Games Rio 2016.

The Integration Test Lab is located within the complex of the Organizing Committee of the Olympic and Paralympic Games in the city of Rio de Janeiro and the structure was responsible for testing systems, applications and the necessary infrastructure for the dissemination of results and carrying out of competitions. Altogether, there are 42 cells that cover each of the sports, as well as 12 specific to the accreditation systems and results information. According to Acts, the laboratory has servers that will distribute information and systems redundancy levels were assured in case of failures. All technology has enabled the transmission of the results to be in real time.

It will be carried out 200,000 hours of technological tests carried out before the opening of the games. This lab is unprecedented and is the last time the ITL will be located in the host city of the Games. It is expected that all the next games IT testing operations in South Korea in 2018, will be conducted entirely in fixed laboratory located in Spain.

To rule out the likelihood of attacks cybercriminals servers laboratory operated in isolation from the network of the main Olympic Complex.

12. **Rio 2016 General Information**

The Canaltech website\textsuperscript{25} released the data of the Rio 2016 in the form of infographic, as follows:

**Fans connected globally**

5 Billion Viewers, 18 web pages billion, 3.5 billion online video views. 1 billion users’ visitors in the official pages of the Olympic Games 2016. 170,000 hours of online content. 130 million hours of video watched on mobile devices.

**Data Centers in the Rio de Janeiro**

300,000 access credentials, 70,000 volunteers, 14,700 records of athletes and medical information. Records and qualifications of 42 Olympic sports and 23 Paralympic sports.

**Cisco UCS servers**

- 163 servers installed with the following functions: Information disclosure system, and Next-generation threat management system.

---

\textsuperscript{23} http://computerworld.com.br/negocios/2014/05/27/cisco-inicia-producao-local-de-servidores-para-comunicacao-unificada/

\textsuperscript{24} http://computerworld.com.br/comite-olimpico-inaugura-laboratorio-de-testes-de-sistemas-para-rio-2016

Information disclosure system - delivering information and real-time results for spectators, commentators and mobile devices.
Next-generation threat management system - providing secure connections for all customers of the Rio 2016.

Locations
- Transportation and processing of 54 million information about the competitions in real time.
- Validation of 9 million tickets.
- 183 support facilities and connectivity to 37 competitions facilities.

The Olympic Village
- 15,000 players connected from 204 countries.
- Triple play services (TV, voice and internet) in the rooms of all athletes.
- Connectivity to 31 buildings and 8000 rooms.

International Broadcast Center
- 150 stations with broadcast rights enabling live broadcasts, which connect billions of fans worldwide.
- 85,000 square meters with 40 CATV channels produced and distributed from the international broadcast center.

Main Media Centre
- 27,000 square meters.
- Allowing news agencies and accredited vehicles make coverage in real time.
- 25,000 accredited media professionals, 9 major international news agencies.
- 50,000 people connected on the go with 273 with internet connection.

Network infrastructure and engineering services
- 8115 products,
- 33,380 hardware modules,
- 440 servers,
- 5,159 points of Wi-Fi access.
- 113,472 LAN ports,
- 177 network security devices,
- 80 systems & applications,
- 18,000 IPS landlines.

Planning, design and implementation support
34,000 hours of planning, design and implementation support, involving 27 engineers, responsible for 54 projects, 900 days of work and 150,000 pages of documentation.

Technical support 24 hours/7 days a week in the center of technology operations of the Rio 2016. 25,732 hours of a team of 65 engineers who have made support for 40 days of local operation.
Reference