Spectrum - The Journal of Operational Applications in Defense Areas

Journal homepage: https://spectrum.ita.br

Quantum Technologies: Quantum Communication

Initiative in Quantum Networks and Their Applications at the Aeronautics Institute of Technology (ITA)

Edison Puig Maldonado[1], André Jorge Carvalho Chaves[1], Rene Felipe Keidel Spada[1], Marcelo Marques[1], Lara Kühl Teles[1], Tobias Frederico[1], Caio Regis Aguiar Moreira[1], Sergio Rebouças[1], Fausto Batista Mendonça[1], Mateus Habermann[1], Vilson Rosa de Almeida[1], Augusto Ribeiro Rodrigues[1], Ingrid David Barcelos[2], Romildo Henrique de Souza[1], Lucio Pinheiro Amaro[1], Renato Machado[1]

[1]Aeronautics Institute of Technology (ITA), São José dos Campos/SP – Brazil
[2]Laboratório Nacional de Luz Síncrotron (LNLS), Centro Brasileiro de Pesquisa em Energia e Materiais (CNPEM), Campinas /SP – Brazil

Article Info

Article History:

Received	29 August	2024
Revised	20 September	2024
Accepted	17 October	2024
Available online	22 October	2024

Keywords:

Quantum information systems
Cybersecurity
Quantum cryptography
Quantum networks

E-mail address:
puig@ita.br (E. P. Maldonado).

Abstract

Professors at the Aeronautics Institute of Technology (ITA) have joined forces to expand their actions in quantum technologies, presenting a proposal to enhance the institution's research capacity in this field. The goal is to have a greater impact on teaching and research activities, support the development of new business proposals, and contribute to education and the popularization of S&T, as well as to the understanding and use of these technologies by Brazilian society.

I. INTRODUCTION

The principles of quantum mechanics, the fundamental theory of physics, applied to the interdisciplinary field currently known as "quantum information," have the potential to revolutionize telecommunications, sensor systems, and computing [1]. Quantum superposition, quantum entanglement, non-cloning, and phenomena such as tunneling have recently enabled a set of mechanisms, devices, and systems that we can call "new quantum technologies" or QT [2,3]. Although it is considered a sensitive area, commercial products based on these new technologies are beginning to emerge. Financial services, telecommunications, logistics, biotechnology companies, and many others are now starting to seek professionals qualified in QT [4,5].

The technological capability to establish quantum data connections represents a qualification requirement for QT. The mastery and implementation of quantum cryptography techniques in these connections, a strategic goal for many countries, governments, and companies, is driving a new market in this field. Quantum key distribution (QKD) techniques [6,7] provide a layer of physical protection that, under ideal conditions, ensures security against various attacks, including potential attacks using quantum computers [8].

Additionally, it is expected that new quantum sensors will soon enable significant advancements in areas of scientific research, metrology, radar techniques, medical imaging, topological visualization (including underground), and environmental monitoring [4]. On the other hand, quantum simulators (controllable quantum systems that can be used to simulate other quantum systems) allow for solving scientific problems that are otherwise intractable, such as modeling the quantum properties of particles, thus addressing issues relevant to materials science and chemistry, among others [9]. Quantum computing (QC) can solve new problems and facilitate the integration of industrial information, such as intensive computing for data analysis. However, this field still faces many challenges, including quantum decoherence problems, qubit instabilities (sensitivity to noise and interference), scalability issues, high resource requirements, and underdeveloped circuit technology [10], thus still limiting many practical applications [11].

This scenario presents new challenges for the country's institutions. At this early stage of the field in Brazil as a technology, it requires intensive joint work at the state-of-the-art level of Brazilian science and engineering.

The Aeronautics Institute of Technology, ITA, is a traditional Brazilian institution that, within its Division of Electronic Engineering, houses the Electronic Warfare Laboratory – LAB-GE [12], an important national reference in academic research in the areas of photonics, electromagnetic materials, radar and other RF and microwave systems, sensors, and secure communication – created in 2001 to support teaching and research in areas of Defense interest, the Specialization Course in Electromagnetic Environment Analysis (CEAAE), and the Graduate Program in Operational Applications (PPGAO). Moreover, ITA has a highly traditional graduate program in physics in Brazil (https://www.pgfis.ita.br/), which began its activities in the 1960s [13], and currently has a faculty active in nanotechnology, nanophotonics, and quantum systems. Thus, ITA possesses significant competencies to operate in this cross-disciplinary field and a culture of dedication to applied projects that can meet the demands of Brazilian society.

This work presents aspects of the initiative being implemented at ITA for a new research infrastructure in quantum data connections, aimed at secure communication, with the goal of enabling new studies, projects, courses, and training. This initiative already has dedicated physical spaces, a group of associated researchers, funding, and institutional support.

II. APPLICATIONS AND DUAL USE

The progress in new quantum technologies for communication, detection/metrology, and computing has accelerated significantly in recent years, driven by improvements in manufacturing, detection, and control technologies, as well as advances in quantum information theory, with new algorithms, techniques, and protocols [14].

Figure 1 shows three main areas: quantum simulation and computing, quantum sensors, and quantum communications, all consisting of unprecedented advancements and capabilities enabled by the laws of quantum mechanics and the properties of quantum states.

Many of the applications of these new technologies are dual-use or are directly employed for military purposes, and they are expected to have strategic and long-term impacts. Military applications of QT will not only offer improvements and new capabilities but will also require the development of new strategies, tactics, and policies, the assessment of threats to global peace and security, and the identification of ethical issues. Considering the TRL (technology readiness level) scale, which defines levels of technological maturity to estimate the state of development and availability for applications, ranging from 1 to 9, most individual new quantum technologies are largely at early TRLs (basic principles observed) up to TRL 6 (technology demonstrated in a relevant environment). However, it is worth highlighting QKD (quantum key distribution) technology, including satellite connections, which is between TRL 7 and 8, with several systems already installed and expected to have a full impact within a few years [15].

Accurate predictions regarding the deployment of these technologies are not possible, as the transition from laboratory studies to real-world applications has, in many cases, not yet begun or is still in progress; even so, experts believe that QT knowledge should be cultivated in the military environment to closely monitor its development and use [15].

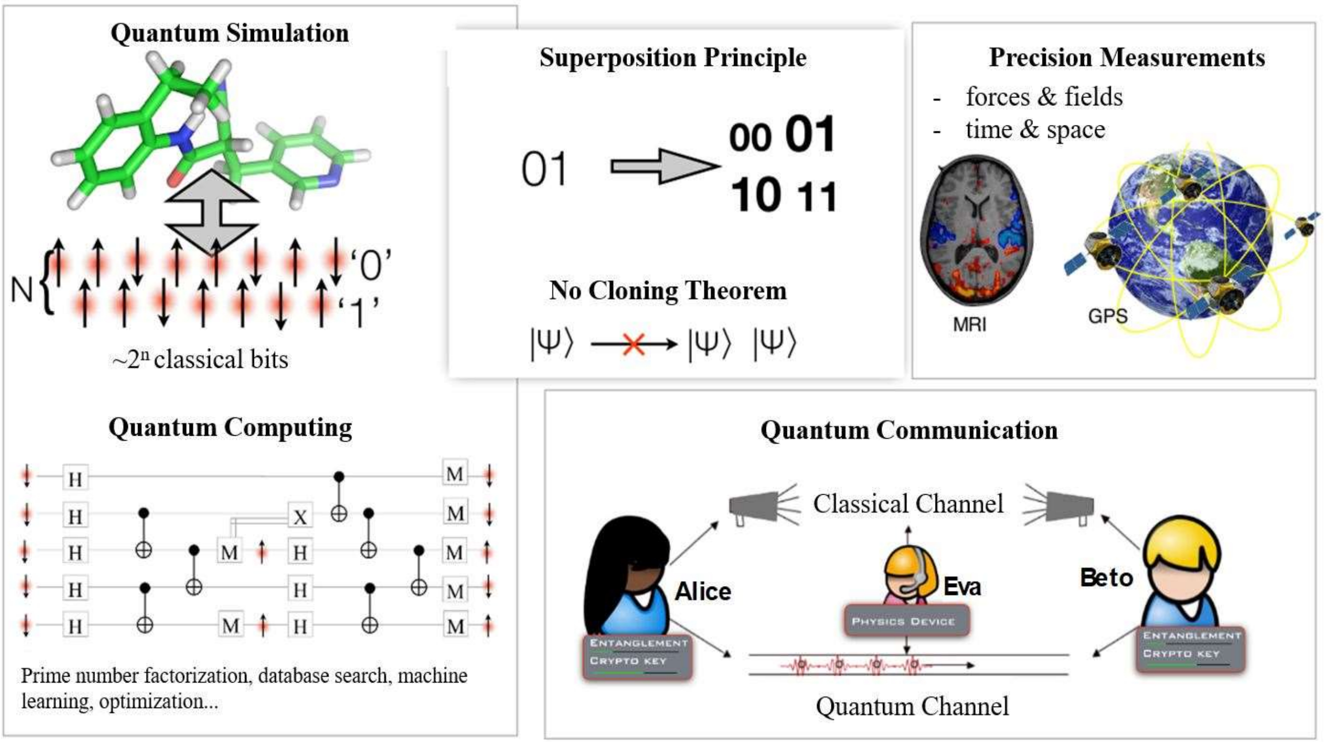

Fig. 1. Main areas of new quantum technologies: quantum simulation, quantum computing, quantum sensors and metrology, quantum communications (edited from "Future Directions of Quantum Information Processing" [14])

III. A PROPOSAL FOR RESEARCH EXPANSION

Together with faculty from the Division of Electronic Engineering (IEE) and the Department of Physics from the Division of Fundamental Sciences (IEF), LAB-GE decided to promote the growth of activities in the QT area at ITA, including scientific and technological research, experimental and model-based developments, and applications in the educational, outreach, and service sectors. The initial goal selected was the expansion of infrastructure and the implementation of quantum data links at ITA using optical fiber (OFC) and free-space optics (FSO), operating with QKD protocols (see Figure 2 for a generic description).

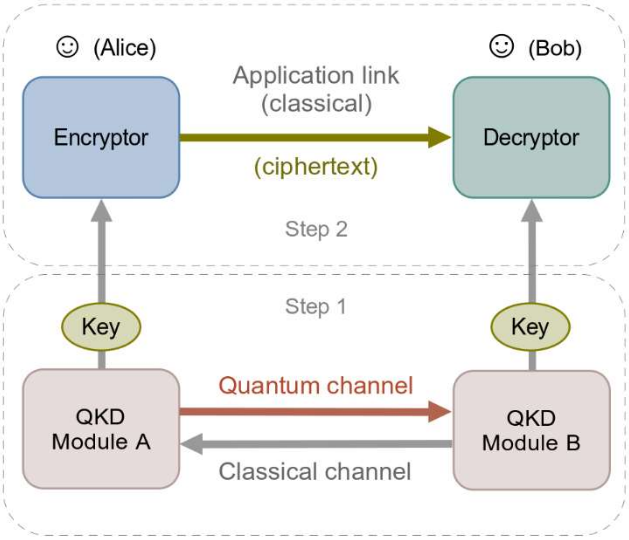

Fig. 2. General diagram of a basic Quantum Key Distribution scheme used in current technology. A secret key is generated by QKD Module A and communicated to the parties, Alice and Bob, with the randomness inherent in quantum states and measurements. Bob remotely receives the key value information through the quantum channel. The No-Cloning quantum property ensures (physically) that this key cannot be copied. Alice and Bob calculate the error rate in the quantum channel by performing a sampling analysis (using the classical channel), diagnose whether the key was communicated securely and (if so) perform some final error correction steps. After carrying out all the protocol steps (including, for example, those described above), Alice and Bob maintain a pair of identical secure keys, which can then be used for tasks such as encrypting messages (e.g. at GHz rates). After a time interval of less than one ms (typically), the key generation and distribution process is restarted (thus renewing the key at a rate of a few kHz).

In its Institutional Development Plan (PDI) [16], ITA defines two priority research lines to which the creation of a center of excellence in QT research aligns: the "Command and control, electronic warfare, and cybersecurity" line and the "Research in Physics, Chemistry, and Mathematics" line. The contemporary and predominantly applied nature of expanding QT research infrastructure will also have a significant positive impact on graduate education, with the potential to support new courses and research activities, especially in the following programs: 1) PG/EEC program, in the area of Electronic Engineering, 2) PG/FIS program, in the area of Physics, 3) PPGAO program, focused on Defense applications. Specific course and training demands from government agencies, institutions, and Brazilian companies, in general, will also be addressed.

This initiative is also aligned with ITA's official Innovation Policy (PI), aiming to modernize education and maintain its excellence, train professionals up to date with sector-specific issues, and offer society solutions for pilot projects, experimental proposals, and training. Specifically, this project represents the implementation of several ITA innovation policies.

Other QT projects will likely be proposed by ITA faculty and researchers in the coming years, such as in the area of quantum sensing. Given Brazil's vast territorial dimensions and the large number of areas to be monitored (such as the Amazon), quantum technologies for environmental sensing represent a future opportunity for the competencies developed through this project, especially for the Brazilian Air Force.

The results of these actions will also provide greater opportunities for technological innovation, enabling Brazilian companies to offer technologically new and/or improved systems and products, as well as new services in this field.

IV. PROPOSAL CHARACTERISTICS

Communication systems containing a quantum channel will be made available to Brazilian society for testing operating regimes, component tests, research of new techniques, training, and demonstrations. These implementations aim to provide ITA with increased research, development, and human resource training in the applications of quantum data networks focused on secure communication, command, control, cybersecurity, and defense. The new infrastructure will be centralized in a new experimental photonics research space for QT at LAB-GE, with the installation of a set of new links protected by QKD, following some of the main protocols currently in use, with characteristics for academic and scientific use in this area and multi-user management. Additionally, it will include the implementation of a new high-performance computing cluster, which will allow ITA to expand studies of advanced processes and devices in QT by the project team and collaborators.

This is a project at the frontier of technological knowledge, particularly based in the fields of photonics and optoelectronics, as well as in materials and techniques in solid-state physics, especially two-dimensional materials. The current project team is highly qualified, experienced, and competent to carry it out, with a team of complementary specialties and impactful work already accomplished in photonics, telecommunications, quantum devices, and quantum computing.

The project was named INFREQUANT – Infrastructure in Photonic Technologies for Quantum Networks and Their Applications in Defense and Security. The new research capabilities will be implemented in multi-user mode, providing supported academic research teams with state-of-the-art communication systems containing quantum channels, available for the study of operational regimes, component testing, investigation of new techniques, training and demonstrations, aiming at secure communication, command, control, cybersecurity and defense.

The project will also include the implementation of a new high-performance computing (HPC) cluster at ITA, which will allow for the expansion of studies of advanced processes and devices for future developments of QKD systems as well as for other QT applications. This new HPC resource will be made available at the Advanced Scientific Computing and Modeling Laboratory (LAB-CCAM) and will consist of one or more new high-performance computing servers (>100 cores, ~512 GB of memory, storage of around 50 TB), in a new data center facility with all the necessary infrastructure.

New postdoctoral and graduate positions are expected to be created at ITA in the coming years due to this initiative. These positions will involve research on topics ranging from the development of learning and education materials to the progressive nationalization of quantum communication systems, as well as research on new devices and techniques, with a predominant focus on engineering

A. Expected Results for ITA

From an institutional perspective, these actions are expected to result in the following achievements:

1) The implementation of a multi-user space for the experimental study of quantum data links could position ITA among the first institutions to make this infrastructure available to Brazilian society, thus supporting widespread research and innovation in this field.

2) The provision of a new high-performance computing cluster will enable new studies in materials and devices for QT, leading to more impactful results.

3) The formation of a team of ITA researchers collaborating in research in this field will initiate a virtuous cycle of knowledge growth, establishing a core of specialists in this region of the State of São Paulo

B. Expected Results for Society

Regarding Brazilian society, these actions are expected to result particularly in the following advances:

1) The offering of technical capabilities that will positively impact new business proposals in this field by Brazilian companies.

2) The training of new human resources specialized in QT, especially at the graduate level, but also meeting the demands of the Brazilian Air Force, Brazilian society, institutions, and companies.

V. SYSTEMS AND MANAGEMENT OF NEW RESOURCES

In the LAB-GE laboratory, an experimental research infrastructure for photonic QT implementations will be established, in a set of rooms that will be called "ITA Quantum Technologies Space" (EQ), managed by a team of researchers from ITA's Division of Electronic Engineering. The target audience includes users (typically scientists and engineers) from ITA, DCTA, other sectors of the Brazilian Air Force, institutions in the areas of defense, security, and science and technology from federal, state, and municipal governments, other public or private ICTs, as well as Brazilian companies.

Proposals will be selected based on evaluations in the following dimensions: 1) scientific, technological, educational, social, and economic relevance; 2) expected impacts; 3) innovation potential; 4) human resource development. Equal opportunities will be ensured for companies and other interested organizations. Supported projects should preferably utilize EQ resources in a shared manner and be executed within the shortest possible timeframe. Only in exceptional cases will projects be allowed to occupy the entire EQ environment and restrict access. Agreements may cover: a) scientific, applied, or technological research, b) extension, c) prototype development for evaluation, testing, or demonstration, d) creation of new products, services, or processes or the improvement of existing ones, e) training, education, and human resource development. The management of each agreement will use a Supporting Foundation as an intermediary and financial-administrative executor.

C. Management Committee

The Management Committee (CG) will serve as the executive body responsible for the operation of the EQ and the definition of its policies. It will consist of the Head of IEE, the Manager and the Deputy Manager of LAB-GE, as well as the Coordinator of the EQ.

The CG will meet periodically to carry out its activities, particularly for schedule approval and monitoring of results. Decisions will be communicated to users and stakeholders through the LAB-GE website. Its responsibilities will include:

• Management of equipment (for free or restricted use).
• Organization of the project selection process and usage schedule.
• Definition of an action plan with recommendations for time allocation for specific types of projects, as well as service provisions.
• Definition of usage allocation policies, following the guidelines of Article 4 of Law No. 10.973, of December 2, 2004 (Innovation Law).

VI. FINAL REMARKS

The new research infrastructure will enable ITA to carry out studies and projects at the state-of-the-art level in the field of quantum data connections aimed at secure communication, as well as for defense, command and control, electronic warfare, and cybersecurity applications. This will consist of an experimental photonics research laboratory within the Electronic Warfare Laboratory – LAB-GE, which will be equipped and have expanded activities to support studies in the field of quantum information.

The expertise gained in the field of quantum data links will contribute positively to the viability of future projects. LAB-GE intends to continue its work in QT with projects that include:

- Expanding the scope of research and development to the field of quantum networks and the quantum internet.
- The potential development of secure communication with satellites, protected by quantum encryption, which would place Brazil among the few nations in the world with this technology.

- Developments in quantum sensor technologies and the engineering of these systems.

The study of new processes, materials, components, and devices usable in new quantum technologies will be enhanced by the expansion of the Advanced Scientific Computing and Modeling Laboratory – LAB-CCAM.

From ITA's perspective, institutional capacity building inquantum data links contributes positively to the viability of future QT projects. The formation of a group of collaborating expert professors will also promote greater activity and impact in ITA's initiatives in the areas of new quantum technologies, and immediately provide new courses and training, new development activities, and graduate-level research in quantum data technologies at ITA.

This initiative also seeks to provide greater opportunities for technological innovation, assisting in the creation of new and/or improved technological systems and products, as well as new services in the area. They will also allow for the high-level training of new human resources specialized in QT, meeting the demands of the Brazilian Air Force and Brazilian society in general.

ACKNOWLEDGMENTS

C. R. A. M. acknowledges the partial support of the National Institute of Science and Technology (INCT-Signals), sponsored by the Brazilian National Council for Scientific and Technological Development (CNPq) under grant 406517/2022-3. V. R. A. acknowledges CNPq for research grants (306389/2021-5 and 403031/2019-2). R. F. K. S thanks the financial support from the São Paulo Research Foundation (FAPESP) grant 2019/07671-4 and CNPq grants 405562/2022-5, 307846/2021-0 and 423423/2021-5. I.D.B. acknowledges the support from CNPq (Grant number 408144/2022-0). T. F. thanks the financial support from CNPq Grant 306834/2022-7 and FAPESP Grant No. 2019/07767-1.

REFERENCES

[1] U.S. Department of Energy. Report of the DOE Quantum Internet Blueprint Workshop. [S. l.: s. n.], 2020. Available at: https://www.energy.gov/sites/prod/files/2020/07/f76/QuantumWkshpR pt20FINAL_Nav_0.pdf.

[2] Gibney, Elizabeth. Quantum gold rush: the private funding pouring into quantum start-ups. Nature, vol. 574, no. 7776, p. 22–24, 3 Oct. 2019. https://doi.org/10.1038/d41586-019-02935-4.

[3] Kantsepolsky, Boris; Aviv, Itzhak; Weitzfeld, Roye; Bordo, Eliyahu. Exploring Quantum Sensing Potential for Systems Applications. IEEE Access, vol. 11, p. 31569–31582, 2023. https://doi.org/10.1109/ACCESS.2023.3262506.

[4] Chen, Sophia. The future is quantum: universities look to train engineers for an emerging industry. Nature, vol. 623, no. 7987, p. 653– 655, 16 Nov. 2023. https://doi.org/10.1038/d41586-023-03511-7.

[5] D. D. Carvalho Brito, R. Pires Ferreira, e A. J. Chaves, “Perspectivas Globais Militares sobre Tecnologias Quânticas”, Spectrum, vol. 24, nº 1, p. 54–60, set. 2023.

[6] Pirandola, S.; Andersen, U. L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; Pereira, J.; Razavi, M.; Shaari, J. S.; Tomamichel, M.; Usenko, V. C.; Vallone, G.; Villoresi, P.; Wallden, P. Advances in Quantum Cryptography. Advances in Optics and Photonics, vol. 12, no. 4, p. 1012, 31 Dec. 2020. https://doi.org/10.1364/AOP.361502.

[7] Gyongyosi, Laszlo; Bacsardi, Laszlo; Imre, Sandor. A Survey on Quantum Key Distribution. Infocommunications journal, vol. 11, no. 2, p. 14–21, 2019. https://doi.org/10.36244/ICJ.2019.2.2.

[8] Lai, Junsen; Yao, Fei; Wang, Jing; Zhang, Meng; LI, Fang; Zhao, Wenyu; Zhang, Haiyi. Application and Development of QKD-Based Quantum Secure Communication. Entropy, vol. 25, no. 4, p. 627, 6 Apr. 2023. https://doi.org/10.3390/e25040627.

[9] Altman, Ehud; Brown, Kenneth R.; Carleo, Giuseppe; Carr, Lincoln D.; Demler, Eugene; Chin, Cheng; Demarco, Brian; Economou, Sophia E.; Eriksson, Mark A.; Fu, Kai-Mei C.; Greiner, Markus; Hazzard, Kaden R.A.; Hulet, Randall G.; Kollár, Alicia J.; Lev, Benjamin L.; Lukin, Mikhail D.; Ma, Ruichao; Mi, Xiao; Misra, Shashank; Zwierlein, Martin. Quantum Simulators: Architectures and Opportunities. PRX Quantum, vol. 2, no. 1, p. 017003, 24 Feb. 2021. https://doi.org/10.1103/PRXQuantum.2.017003.

[10] Sood, Sandeep Kumar; Pooja. Quantum Computing Review: A Decade of Research. IEEE Transactions on Engineering Management, vol. 71, p. 6662–6676, 2024. https:// doi.org/10.1109/TEM.2023.3284689.

[11] Lu, Yang; Sigov, Alexander; Ratkin, Leonid; Ivanov, Leonid A.; Zuo, Min. Quantum computing and industrial information integration: A review. Journal of Industrial Information Integration, vol. 35, p. 100511, Oct. 2023. https://doi.org/10.101 6/j.jii.2023.100511.

[12] LAB-GE, Laboratório de Guerra Eletrônica, https://www. ele.ita.br/~labge/

[13] APG-ITA, Associação de Pós-Graduandos do Instituto Tecnológico de Aeronáutica História da Pós-Graduação no ITA, https://apgita.org.br/wp-content/uploads/2019/08/Historia_da_ pos _graduacao.pdf

[14] Lloyd, Seth; Englund, Dirk. Future Directions of Quantum Information Processing. VT-ARC. [S. l.]: Virginia Tech, 2017.

[15] Krelina, Michal. Quantum technology for military applications. EPJ Quantum Technology, vol. 8, no. 1, p. 24, 6 Dec. 2021. https://doi.org/10.1140/epjqt/s40507-021-00113-y.

[16] Instituto Tecnológico de Aeronáutica, “Visão e Futuro - Plano de Desenvolvimento Institucional 2021-2023”. [Online]. Avaiable: http://www.ita.br/pdi.