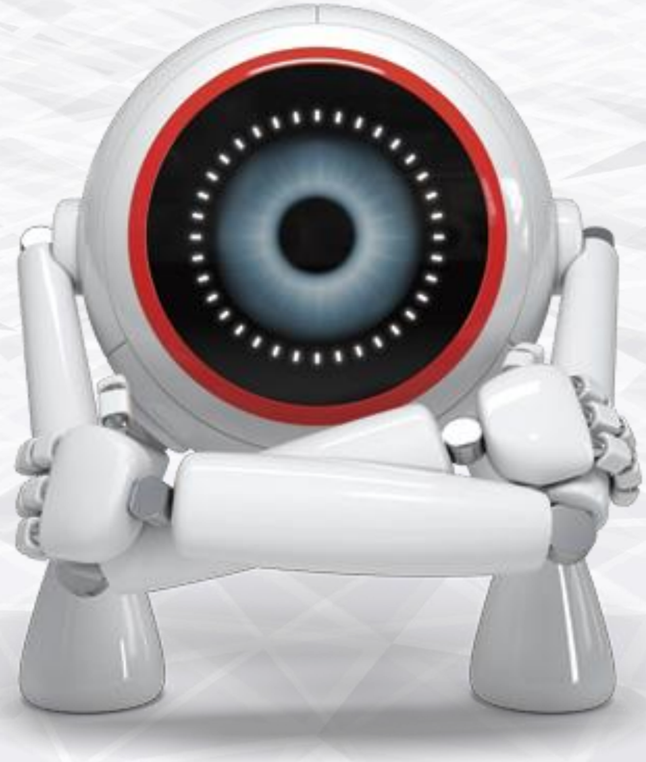
bradesco | Fornecedores

INFORMATION SECURITY

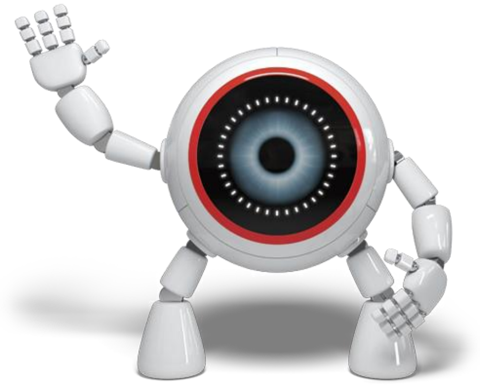


The purpose of this booklet is to disseminate knowledge to service providers on the topic of Information Security and Cybersecurity.

It is imperative that Suppliers and/or Business Partners who have access to Information Assets ensure compliance with all applicable legislation on Information Security, privacy and data protection, including (where applicable) the Federal Constitution, Consumer Defense Code, Civil Code, Civil Rights Framework for the Internet (Federal Law No. 12.965/2014), its regulatory decree (Decree 8.771/2016), the General Data Protection Law (Federal Law No. 13.709/2018) and the Regulatory Agency BACEN - Central Bank of Brazil.

We count on you.

Good Reading!



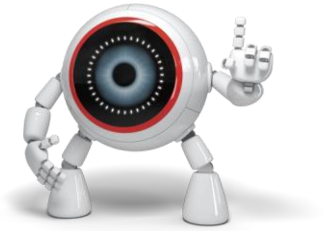
In times of instant information sharing, we spend more time connected.

On the other hand, exposure to cyber threats and attacks increases.

Cybercriminals have started to keep an eye on this context and exploit loopholes to run scams, trying all the time to steal confidential information from people, companies and governments in order to gain advantages or even ruin businesses.

These attacks may result in data leaks and business disruption, causing damage to companies' image, finances or even assets.

Bradesco has always been concerned about security, including the process of hiring our Suppliers and Business Partners.



Your commitment is essential if we are to continue to keep our Organization secure!

Stay up to date!

The Organization has a Corporate Information Security and Cybersecurity Policy, which governs us in implementing best practices.

Clique aqui e conheça as diretrizes!

Do you know the pillars of Information Security?

Information Security is made up of 3 pillars:

Processes
These are sets of actions with a common purpose - Rules and Standards.

Technology
Tools, applications and infrastructure used to execute or support processes - Monitoring, Antivirus, firewall, corporate network, among others.

People
Those who manipulate, verbalize and transport the information - Awareness and training.

You are essential to ensuring Information Security!

THREATS

Know the cyber threats to which companies and people are exposed:

Spyware

Program that monitors computer activities.

Virus

Any malicious computer codes with the aim of damaging machines and computer programs and/or stealing information. Worm-type viruses have the ability to spread to other computers on the network.

Trojan Horse

Apparently harmless files, but they contain malicious codes (viruses) that are installed when the file is opened. These codes can give crackers easy access to break into the system and steal information.

Phishing

These are messages, in the name of companies/official agencies, inducing the victim to access fake pages to steal information. Texts, images and links very similar to real ones are used to obtain confidential information, such as passwords and personal data.

Ransomware

Type of malicious code that restricts access to infected systems/files, whose authors demand payment of a "ransom" to restore them. This attack, which usually occurs by sending emails containing an attachment or link with malicious code, can result in data leakage and business interruption, causing financial, image and reputation losses.

SOCIAL ENGINEER

A scammer who uses methods and techniques (computer and psychological) aimed at manipulating and persuading a certain person to reveal personal data or corporate information, or to jeopardize computer systems to do so. They contact the victim and exploit their weaknesses, such as naivety, greed, fear, curiosity, among others, to obtain information and commit crimes.

STAY TUNED!

"Social engineers" often bug public places, rummage through garbage in search of documents and, above all, monitor their victims' activities on social networks. For this reason, proper disposal of physical documents (papers, folders, etc.) and careful Internet browsing are of the utmost importance.

Avoid talking about professional and internal matters of the Bradesco Organization in public places, such as parties, restaurants, cabs, among others.

Always confirm the identity of the person you are speaking to, especially if the contact is remote, for example on the phone, email, among others. Never give out passwords.

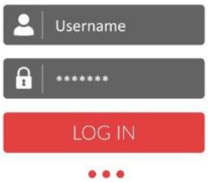
Ensure the authenticity of messages received, regardless of the sender or subject.

Do not click on links or execute files attached to suspicious messages received by email or SMS.
The same applies for apps: don't install apps from incoming links - use official platforms.

In case of suspicion, do not proceed with any of the instructions; send the message to **evidencia@bradesco.com.br** and delete it from your computer (press SHIFT + DEL).

VULNERABILITY

Weaknesses that expose us to threats and, when exploited, may cause damage. Some examples that should be avoided:



Password sharing.

Workstations unlocked.

Improper disposal of documents.

Abandonment of documents in printers or on tables.

Access to company premises without identification and authorization.

Note that vulnerabilities may occur in both digital media (computers and cell phones) and physical media (documents and workplaces).

Therefore, we need everyone's commitment!

RISK

Information Security Risk is associated with the exploitation of one or more vulnerabilities, with a negative impact on the business.

Not only businesses are exposed to risks, such as data leaks and their consequences.

Can you imagine if your social network was hacked?

Or if your cell phone is stolen?

This can have consequences, such as the exposure of your personal data, telephone contacts, messages and photos, causing damage to your image and enabling the use of data in illicit practices.

How to protect information???

Through security mechanisms, such as:

- Encryption;
- Antivirus;
- Security Copies (backups);
- Logical Access Control;
- Physical Access Control;
- Access Segregation;
- Information Security Awareness and Education.

TAKE NOTE!
Tips for protecting information

Equipment for work activities must contain security mechanisms that ensure the confidentiality, integrity and availability of information accessed, stored, processed and/or transmitted. Remember to store them in a safe place.

When you are away, lock your workstation.

For virtual meetings, only use approved software, always identify yourself when joining the meeting and make sure that only invited people are participating.

Information from the corporate environment must not be extracted, copied, published or shared with unauthorized people or channels.

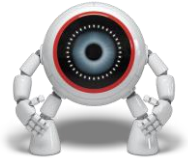
Use professional email exclusively for work-related matters.

CONFIDENTIAL

Information must always be classified and labeled considering its value, legal requirements, sensitivity or criticality.

Your password is personal and non-transferable. Create strong passwords: combine letters, numbers and special characters.

Review/management of access to information must be carried out periodically. Users should only be granted the access and resources that are strictly necessary and essential for the performance of their activities.



TAKE NOTE!
Tips for protecting information

Immediately remove the documents from the printer and copier.

When disposing of physical documents, remember to shred or tear them up using a paper shredder, for example.

Be careful and critical when posting information about yourself and your family on social media. Exposure can attract malicious people and criminals.

Always confirm the identity of the person you are speaking to.

When you receive offers of products or services, make sure that the information provided is legitimate and trustworthy. If in doubt, contact the company's official channels.

Do not click on links or execute files attached to suspicious messages. Forward to evidencia@bradesco.com.br and then delete it.

Have implemented business continuity processes to ensure that, in the event of incidents, operations remain in an appropriate state until the normalization of activities.

TAKE NOTE!
Tips for protecting information

Where applicable, ensure that certifications are in place to keep compliance with the quality standards of all the company's processes.

In the event of any information or cyber security event or incident, contact the Bradesco Organization.

Want more security tips?

Access: **seguranca.bradesco**

Central falsa

O banco não entra em contato **pedindo senhas** ou códigos da **Chave de Segurança**.

DISPOSITIVOS DE SEGURANÇA

Praticidade e proteção ao seu alcance

CANAIS DIGITAIS

Opções de atendimento com a comodidade que você precisa

SEGURANÇA DA INFORMAÇÃO

Como protegemos as informações de nossos clientes

So long!

bradesco | Fornecedores

bradesco | Fornecedores

INFORMATION SECURITY