

## **Information Security Guide**

### **Security Slopes**

### **CHANNELS**

#### **INTERNET BANKING AND CUSTOMER SERVICE**

- Make sure that you are not being observed while entering your personal financial data (password, card code or Token) on our transactional Internet page.
- Create different users for your company: a query access for your designated personnel and another one of greater responsibility, for you, who is the one who manages the payments.
- Make sure you are not overheard if you confirm your financial details via Customer Service.
- Provide your financial data only if you have initiated the contact and when it is essential to obtain a service in return (authenticate virtual purchases or remote payments, to establish the physical shipping address for your electronic purchases, etc.).
- If, during a call, you do not correctly complete the validity of your financial data, you will be referred to the nearest branch, as a protection measure against the possible usurpation of your identity.
- POINT OF SALE
- Make sure that you are not observed while entering or disclosing your personal financial data (PIN, secret code, card code or Token) when making your payments.
- When paying with your debit or credit card(s), be prudent and cautious about who you are giving or disclosing it to, if the contact is by phone. Make sure it is staff of the establishment.
- Always keep an eye on your debit or credit card(s).
- When making purchases through the Internet, be sure to read and agree with each one of the terms and conditions required by the establishment in which you are going to buy.
- When you move from one cashier to another to swipe your debit or credit card in case the POS device is broken, make sure there are no crowds around you when you enter your PIN.