



## **RESEARCH ON COMPUTER SECURITY IN PERUVIAN ORGANIZATIONS DATA SHEET**

**Lima, August 2006**

The research describes the state presented by private and public organizations in Peru in regards to computer security. It includes a review of the use of policies and procedures, ownership of hardware, software and solutions, and finally the investment that will be made in the IT business segment. The research is based on a structured questionnaire with 85 questions related to the subject of security addressed to the people in charge of systems in the country's main organizations.

### Objectives

1. To determine the current situation of security systems in Peru's organizations.
2. To analyze the vulnerability of Peruvian companies.
3. To identify the leading brands for systems security in the market.
4. Business Opportunities

### Population under study and sample

Large and medium corporate companies and, main government organizations in Peru belong. According to the segmentation criteria of Dominio, all those organizations whose annual revenues exceed \$ 40 million American dollars are part of the large corporate segment. The medium ones have an income between 1 and 40 million. Estate organizations have been identified on a case by case basis with organizational charts from the public sector.

Samples have been separately analyzed for each segment in order to maintain sampling errors within the suitable limits for market research. This sampling strategy allowed us to obtain a total margin of error of only 3.9%, i.e. 22% below the universally accepted margin error in market research.

The population structure, the number of organizations by segment, sampling sizes and the sampling errors can be seen in the following chart:

Segment	Population	Sample	Expected margin of error
Corporations and large companies	309	150	5.7%
Medium companies	8691	320	5.4%
Main governmental organizations	208	120	5.8%
<b>Total</b>	<b>9208</b>	<b>590</b>	<b>3.9%</b>

### Variables under study

- Policies and security procedures.
- Market Share of different brands such as suppressors, UPS, stabilizers, antivirus, antitroyanos, backup devices, firewalls, Antiadware, among others Antispyware.
- Having teams that provide security against fire and power failure.
- Having solutions that avoid or reduce the most common threats, such as virus, trojans, adware, spyware, phishing, pharming, keyloggers.
- Update patches for operating systems and applications.

- Make Backups (frequencies, means, and place of storage).
- Holding Disaster Recovery solution.
- Authentication of users and emails.
- Holding levels of access to files
- Having content filtering solutions.
- Tenure security in laptops.
- Having Firewalls.
- Having IDS / IDP.
- Analysis of the behaviour of all members of the organization against information security within the organization.
- Trend and rate of investment in security budgets.
- IT.
- Vulnerability towards various types of security threats and incidents.
- Incidents experienced during 2005.
- Perceptions about safety products that provide Cisco, D-Link, Computer Associates, Hewlett Packard, IBM, Linux, Microsoft, Novell, Oracle, Sun, Sybase and Unix.
- Outsourcing security.