

PRODERJ



10

STRENGTHENING THE BARRICADE

Proderj invests heavily in Risk Management to identify demands for protection and to add agility and integrity to its services.

Detecting vulnerabilities in infrastructure and creating actions to eliminate them are some of the current challenges faced by Proderj, the Rio de Janeiro State Information Technology and Communications Center, in the Information Security area. This governmental body has launched a project aiming to identify options for improving its



About Proderj

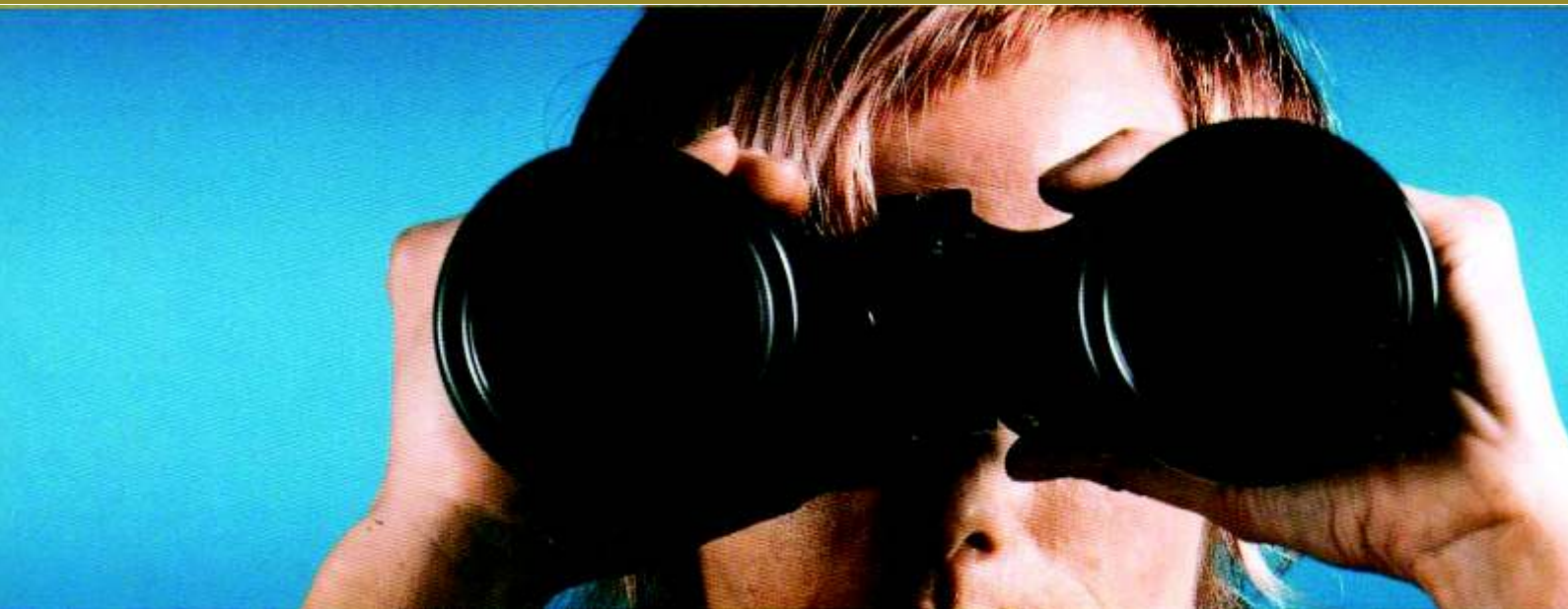
The organization operates basically in four areas: Electronic government, technological infrastructure, modernization of public management, and digital inclusion. For the latter, Proderj runs the Community Internet Program, created approximately three years ago for the purpose of promoting the democratization of Internet access. There are currently 51 community Internet centers maintained by the organization in several locations of the state of Rio de Janeiro, serving more than 820,000 people. Regarding technological infrastructure, Proderj acts as liaison between the several bodies of the state government. "If the police need to access the State Treasury to search for any specific information, they need to connect to Proderj, which mediates the exchange of information," explains Mendes. These examples mentioned by the CIO demonstrate the organization's demand for more efficient and precise risk control.

technological infrastructure and therefore to prevent losses, attacks and unauthorized access to confidential information, rendering both assets and components more reliable and enhancing service robustness.

Sérgio Mendes, Proderj's CIO, reveals that the mobilization for strengthening their security strategy gained life after a number of penetration and website graffiti attempts and attempts to deliver phony e-mails to collaborators using addresses of state departments. "The first effort to solve the problem took place in April last year, when the Information Security Committee was created to manage risks, says Mendes. Considering that Proderj provides technological infrastructure support to several of the state's agencies, it is naturally responsible for a large amount of confidential data which cannot be intercepted or modified without clear authorization. Information on payments to personnel employed by the state of Rio de Janeiro, active debt, auto theft data, taxes and public school enrollment are among the numerous examples of data requiring protection and proactive actions.

PRESERVATION OF THE INFRASTRUCTURE

After identifying the need to acquire a risk assessment and knowledge management tool, Proderj carried out a bidding process which was won by Módulo and its Módulo Risk Manager™ tool. According to Mendes, the requisites for using the software defined the cycle of benefits which were soon to be experienced, since the implementation of the tool immediately required an inventory of all the



technological assets maintained by the organization, and this promoted a significant rearrangement of its internal infrastructure.

By producing an inventory, we managed to clearly define a formal framework of the responsibilities for each technological asset. Simply defining who is in charge of what solved nearly 90% of our infrastructure-related problems, in addition to having resolved several internal conflicts across management areas. Now, each one knows exactly what is and what is not within the scope of their work, and each area is expected to protect assets under their custody”, celebrates the CIO.

The inventorying process took nearly two months to be completed. According to Mendes, each department of the organization was assigned the responsibility for specific assets, regardless of the types of software run in each different piece of equipment. “This also provided us with higher integration across management areas, which found themselves forced to work together to keep the assets under their responsibility functioning perfectly”, he says.

In this context of assignment of responsibilities, Proderj created the “Assets Management Standard”, published by the Official Gazette, which introduces concepts such as 'owner' and 'custodian', two different levels of responsibility for technological assets.

For these reasons, one can say that

although it was not the original intention, implementing the Risk Manager tool brought management functionality to Proderj, which is of the utmost importance to the organization’s huge structure, consisting of three data centers, one of them equipped with a mainframe and 15 servers while another one has more than 60 servers.

RECOVERY PLAN

The first risk assessment in which Proderj used Risk Manager was carried out at the institution’s Community Internet Centers (Centros de Internet Comunitária - CICs) and in its digital inclusion laboratories, whose purpose is to offer the population free, broadband Web access. “We found out which technological assets were capable of supporting the CIC structures and outlined a big picture. Next, we managed to sensitize Proderj’s higher management about the relevance of treating their assets”, says Mendes.

In this particular case, the risk assessment was essential to demonstrate the impact of the lack of security on the final results presented by Proderj. Thus, each one of the organization’s 10 technological assets were defined separately. Among them, Proderj’s CIO mentioned two examples: an analysis of connectivity elements, in which a risk of approximately 57% was attested; and database assets assessment, which showed a risk of approximately 52%.

To reverse the picture, the security

By producing an inventory, it was possible to clearly define the responsibilities for the technological assets.

committee defined a specific action plan for each management area, aiming to eliminate, within a 30-day period, the risks regarded as very high. For this purpose, the committee used Risk Manager to issue an "Operational Risk Report" containing tables with security controls that should be implemented.

As to the database asset, several controls were listed by the risk assessment tool, such as using cryptography for remote management of the application, preventing the use of programs that allow users and passwords on the system's process list to be viewed. After performing all the implementations recommended, the risk of the asset dropped from 51.94% to 50.17%. The reduction may seem irrelevant, but the rationale is that, as Mendes explains, there are several components in a single asset, and as long as the software applications still bear risk, the final result of the asset as a whole is impacted. As to connectivity assets, for example, the risk started at 57.04% and was lowered to 37.88%, an average that reflects the drop in risks

The campaign started with the publication of the security policies and standards of the organization. A presentation was made to the managers, which were assigned the task of replicating the information to their subordinates. These should, after gaining awareness of the standards, sign a term of responsibility to be kept in each employee's personnel file. This routine is still adopted whenever a new employee joins the Proderj staff.

The initiative yielded positive results regarding the assimilation by collaborators of security-related information considered essential. It also made it possible for collaborators to voice their suggestions and reservations concerning the existing Information Security Policy, which has motivated its improvement and made it increasingly aligned with users' profiles, as well as with the organization's. "Collecting and organizing this information has only been possible with the use of Risk Manager", highlights Proderj's CIO.



One of the **strategies** adopted by Proderj to **prevent risks** was to assess the dissemination of an **Information Security** culture among employees.

regarding most components.

One of the strategies adopted by Proderj to prevent risks detected by Risk Manager was to evaluate the dissemination of an Information Security culture among employees. For this purpose, a panel containing the organization charts of the institution was created, in which it is possible to clearly see the risk in each area based on a survey of collaborators' habits. "When we presented the results of this survey, we demonstrated to the employees how vulnerable their organization was, which mobilized them a great deal around the importance of preserving the security of their information. The users were not familiar with Proderj's security policies, although they were published in 2001. Therefore, based on this assessment, we realized that our risk index was too high and decided to launch a comprehensive awareness campaign, Mendes recalls.

REAPING THE HARVEST

Sérgio Mendes emphasizes that the great merits of this project were the possibility to surgically attack the risks found, the integration promoted between the organization's different areas, which started to work together to reduce the risk of certain assets, higher employee awareness, and the significant improvement of Proderj's technical capacity using this risk assessment tool. "We have become specialists in using the Risk Manager and now we are able to provide consulting to any of the state's government bodies, both for assessing risks and for implementing the recommended controls, which is pretty difficult," he concludes.