



CYBERWELLNESS PROFILE

REPUBLIC OF PERU



BACKGROUND

Total Population: 29 734 000

(data source: [United Nations Statistics Division](#), December 2012)

Internet users, percentage of population: 39.20%

(data source: [ITU Statistics](#), December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- [Penal Code](#)
- Computer Crimes Act
- Incorporating Computer Crimes in the Criminal Code.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Protection of Personal Data - [Digital Signatures and Certificates Law](#).

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Peru has an officially recognized national CIRT known as [PeCERT](#).

1.2.2 STANDARDS

There is no officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Peru.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Peru has an officially recognized cybersecurity strategy known as [Plan Estratégico en Seguridad Informática y de la Información](#).

1.3.2 ROADMAP FOR GOVERNANCE

Peru does not have a national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY

The [PeCERT](#) and the Division of High Technology Crimes (DIVINDAT) are responsible for cybersecurity in Peru.

1.3.4 NATIONAL BENCHMARKING

Peru does not have an officially recognized national benchmarking or referential to measure cybersecurity development.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no program or project for research and development of cybersecurity standards, best practices and guidelines.

1.4.2 MANPOWER DEVELOPMENT

DIVINDAT and PeCERT actively train their personnel to maintain and develop their capacity to perform their core functions. Internal awareness raising initiatives within their own institutions have entailed a full range of activities to ensure users' understanding of concepts not always associated with but key to cybersecurity such as physical security, security logic, and human security. External awareness raising activities have included media campaigns, and outreach and education for private sector entities including banks, payment processors, and other business and commercial interests. Awareness raising campaigns have also targeted citizens at large, emphasizing basic good practices for reducing vulnerability and protecting one's identity and information while using the Internet and ICTs.

1.4.3 PROFESSIONAL CERTIFICATION

Peru does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Peru does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states DIVINDAT actively seeks assistance from foreign entities where and when appropriate. It also maintains active partnerships with and supports the efforts of national and international NGOs working to combat cyber and other crimes that have utilized ICTs.

1.5.2 INTRA-AGENCY COOPERATION

Peru does not have an officially recognized national or sector-specific program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

[PeCERT](#) has initiated a dialogue to increase collaboration with the private sector, particularly ISPs and banks.

1.5.4 INTERNATIONAL COOPERATION

Peru is a member of the [ITU-IMPACT](#) initiative and has access to relevant cybersecurity services. Peru also participates in the [OAS CICTE](#).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

-[Articles 181-A*](#) and [183-A*](#) of the Criminal Code, added by the law n. 28.251 from April 1991.

2.2 UN CONVENTION AND PROTOCOL

Peru has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the [Convention on the Rights of the Child](#).

Peru has acceded, with no declarations or reservations to articles 2 and 3, to the [Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography](#).

2.3 INSTITUTIONAL SUPPORT

There is no information about any agency responsible for child online protection in Peru.

2.4 REPORTING MECHANISM

[PeCERT](#) provides an email to report incident: pecert@pcm.gob.pe.

DISCLAIMER: Please refer to <http://www.itu.int/en/Pages/copyright.aspx>

More information is available on ITU website at <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx>

Last updated on 19th February 2015