

CNPIC

The National Center for Critical Infrastructure Protection (CNPIC) is the director and coordinator of all activities related to Critical Infrastructure Protection entrusted with the Secretariat of State for Security of the Ministry of the Interior, which is attached.



[back](#)

SCADA Guides

SCADA systems or systems for Supervisory Control and Data Acquisition, comprise all application solutions that set out measures operational data from local and remote control equipments.

The data is processed to determine if the values are within tolerance levels and, if necessary, take corrective action to maintain stability and control.

The security of SCADA systems is especially relevant in the field of Critical Infrastructure. A failure in critical infrastructure would undermine the whole society, in many cases for an entire country and its environment. Safety is beyond the scope of the undertaking and requires the advice and supervision of higher organisms.

Guía 480 SCADA - Seguridad en sistemas SCADA	Versión 03-2010
Present the issues raised by the SCADA systems and their vulnerabilities, their impact and the imperative to control their security	[Download]
Guía 480A SCADA - Guía de buenas prácticas	Versión 03-2010
Get a deep understanding of the risks facing the business from threats of process control systems to identify and bring them to the appropriate level of security protection that is required.	[Download]
Guía 480B SCADA - Comprender el riesgo de negocio	Versión 03-2010
Based on the reasons explained in the guide CCN-STIC-480A provides guidance to study business risk and continuous study of this risk.	[Download]
Guía 480C SCADA - Implementar una arquitectura segura	Versión 03-2010
Based on the reasons explained in the CCN-STIC-480A provides guidance in deciding a proper security architecture for process control systems.	[Download]
Guía 480D SCADA - Establecer capacidades de respuesta	Versión 03-2010
Based on the reasons explained in the CCN-STIC-480A provides guidance for establishing response capabilities related to threats to digital security of process control and SCADA systems.	[Download]
Guía 480E SCADA - Mejorar la concienciación y las habilidades	Versión 03-2010
Based on the reasons explained in the CCN-STIC-480A, is developed by examining in detail each of the key areas to provide overall guidance on improving safety skills in the control of processes within organizations.	[Download]
Guía 480F SCADA - Gestionar el riesgo de terceros	Versión 03-2010
Based on the reasons explained in the CCN-STIC-480A provides guidance on good risk management practices of third parties for the safety of process control systems.	[Download]
Guía 480G SCADA - Afrontar proyectos	Versión 03-2010
Based on the reasons explained in the CCN-STIC-480A, provides good practice guidance on how to include security considerations in security projects in process control.	[Download]
Guía 480H SCADA - Establecer una dirección permanente	Versión 03-2010
Based on the reasons explained in the CCN-STIC-480A, provides guidance to define and implement appropriate governance frameworks for security in process control systems.	[Download]


[back](#)

Alerts and advisories of vulnerabilities (source ICS-CERT)

- [Acces alerts and advisories](#)

[back](#)

Documentation

- [Directory of Critical Infrastructure Protection](#) 
- [Guide of Good Practices of cybersecurity in Industrial Control Systems](#)