



Instrucciones para la auto-evaluación de los Controles Críticos de Ciberseguridad:

Planilla de medición de los Controles Críticos de Ciberseguridad:

http://www.cert.gov.py/index.php/download_file/view_inline/1375

La evaluación debe incluir a toda la organización: redes, sistemas, equipos, aplicaciones, procedimientos, datos y personas. Para poder realizar esta evaluación es necesario involucrar a todas las áreas involucradas, de modo a asegurar que las respuestas sean lo más certeras posibles.

La evaluación consiste en identificar de manera cualitativa el grado de implementación de cada sub-control de la guía, de acuerdo con la siguiente escala:

- **0 - Nulo:** el sub-control no existe
- **1 - Básico:** el sub-control existe a nivel de procedimiento (escrito o manual) y se cumple parcialmente
- **2 - Intermedio:** el sub-control existe de manera más o menos automatizada (mediante una herramienta tecnológica) y se cumple parcialmente
- **3 - Avanzado:** el sub-control existe de manera completamente automatizada (mediante una herramienta tecnológica) y se cumple completamente
- **4 - Completo:** el sub-control existe de manera completamente automatizada, se cumple completamente y se monitorea regularmente para controlar su funcionamiento correcto

Se debe tener en cuenta que para considerar que un sub-control existe de manera completa (nivel 4) debe haber una política formal que lo contemple, debe estar implementado en toda la red, sistema, aplicación, equipo, dato y/o procedimiento que aplique, y debe haber una persona, área y/o herramienta que se asegure que el sub-control se encuentra implementado y que funciona como se espera. Por ejemplo, un sub-control que se ha implementado en algunos sistemas pero que no se encuentra soportado en una política formal y/o que no se ha implementado en todos los sistemas sólo podrá puntuar como un cumplimiento intermedio (nivel 2), debido a que corresponde a un cumplimiento parcial. En caso de que el sub-control ha sido aplicado a algún sistema por iniciativa de una sola persona se considera que el nivel de cumplimiento es nulo (nivel 0), ya que se trata de una acción esporádica y muy limitada. Para considerar un cumplimiento básico (nivel 1) es necesario que, como mínimo, exista una persona responsable del control (aunque sea de facto) y que, de manera más o menos regular, lo implemente donde corresponda.

Para el cálculo del porcentaje de cumplimiento se utiliza una escala ponderada, la cual asigna un peso mayor a aquellos sub-controles básicos y más importantes y un peso menor a aquellos menos críticos. El cumplimiento completo de todos los sub-controles básicos (Control 1 al 6) asegura un nivel de cumplimiento de 85%.