

Principios institucionales de seguridad de la información

INTRODUCCIÓN

El Instituto Nacional de Estadística y Geografía (INEGI) reconoce como activos importantes a la información estadística, geográfica y de gestión institucional, así como los datos personales de los trabajadores, de los informantes y de los usuarios, ya sean propiedad del Instituto o confiados por terceros; este reconocimiento tiene sustento formal en el marco normativo que rige sus actividades.

En cuanto al entorno en la materia, en fechas recientes se han incrementado a nivel mundial los ataques a los acervos de información de diversas instituciones, como: la banca privada, los gobiernos locales y nacionales, las agencias de noticias y las universidades, entre otras.

Por ello, resulta necesario reforzar, de manera sistémica, el cuidado de la información que el Instituto capta, integra, produce, difunde y resguarda, así como los datos personales de los trabajadores, de los informantes y de los usuarios.

OBJETIVO

Establecer un ambiente de seguridad de la información que mantenga la integridad, la confidencialidad y el acceso a la información, todo ello de manera inherente a los procesos de trabajo.

PRINCIPIO GENERAL

Es responsabilidad de las unidades administrativas y de cada servidor público del INEGI resguardar la información en el ámbito donde se desenvuelven.

PRINCIPIOS ESPECÍFICOS

- Aplicar los procedimientos específicos de cada proceso de trabajo, así como aquellos de carácter transversal, para cuidar la información, lo cual implica:
 - Asegurar su confidencialidad, permitiendo el acceso sólo al personal autorizado, evitando la sustracción indebida.
 - Garantizar su integridad, evitando la pérdida, daño o alteración.
 - Asegurar su disponibilidad a los usuarios autorizados en el momento en que lo requieran.
- Considerar los datos personales de los trabajadores, de los informantes y de los usuarios como información confidencial.
- Asegurar que los visitantes a las instalaciones del Instituto, que requieran acceder a la información, conozcan y cumplan con estos principios institucionales de seguridad de la información.
- Alertar a los responsables de los procesos de trabajo sobre situaciones del entorno que pudieran afectar el resguardo apropiado de la información, comprometiendo su confidencialidad, integridad o disponibilidad.
- Prevenir a los responsables de los procesos de trabajo, en relación con la información, cuando por accidente o acción deliberada (ante evidencia o mera presunción):
 - Se comprometa su confidencialidad al ser accesible a extraños.
 - Se pierda, dañe o altere.
 - Se obstruya su acceso al personal autorizado, ya sea para consulta o actualización.

Aguascalientes, Ags., mayo de 2012